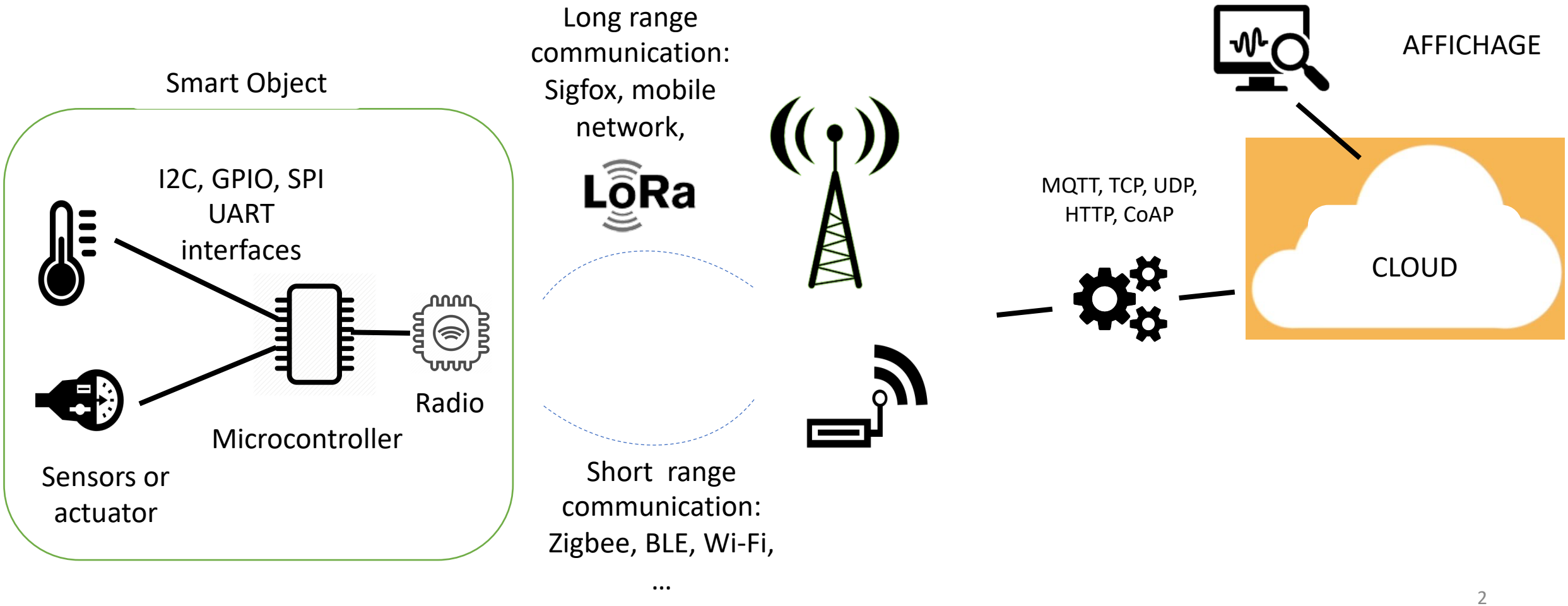
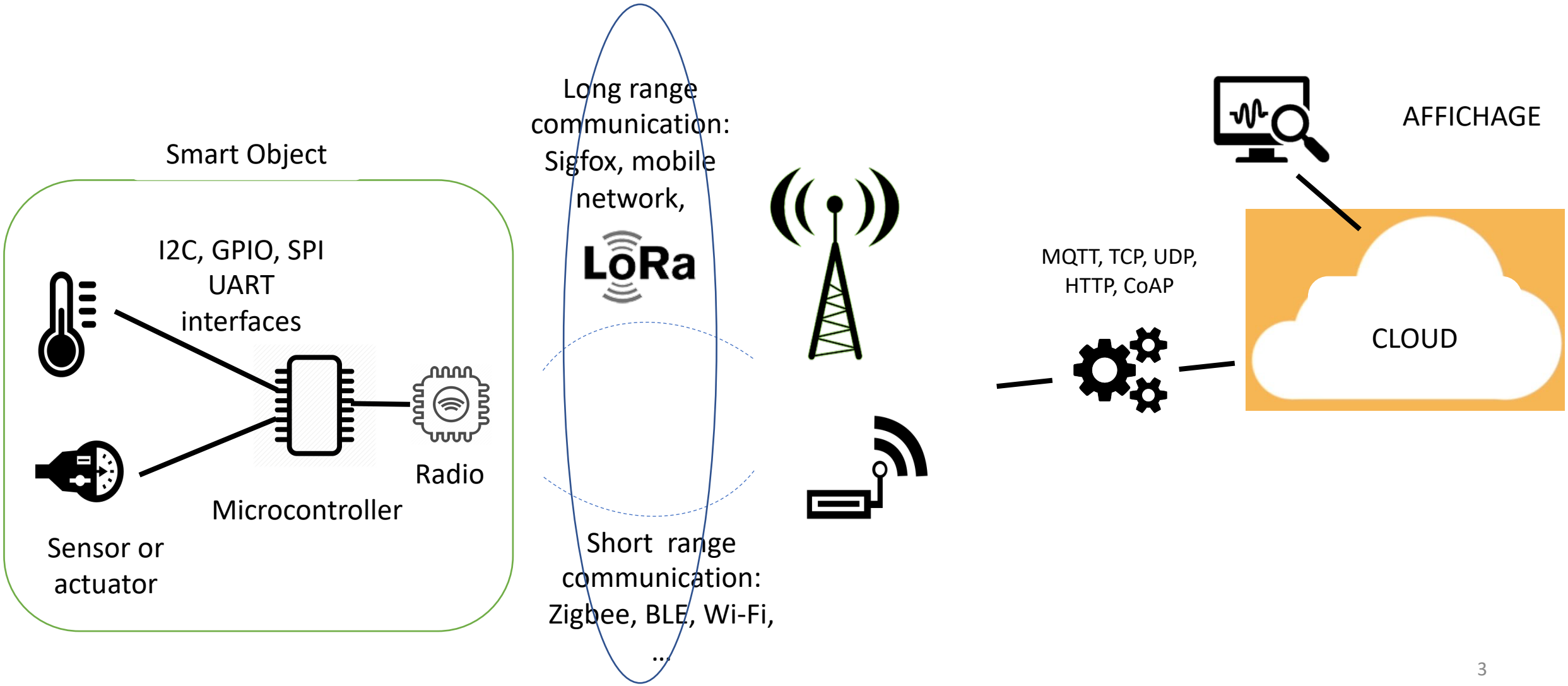
Internet of Things: short range vs long range communication

Kamal Singh, MCF Telecom ST-Etienne

General plan



General plan



References

- MOOC Programmaer l'nternet des objects https://www.fun-mooc.fr/courses/course-v1:MinesTelecom+04038+session01/info
- MOOC Explorer la 5G : Xavier Lagrange https://www.fun-mooc.fr/courses/course-v1:MinesTelecom+04035+session02/info
- Cours Michel Courbon
- Mobilefish, YouTube https://www.youtube.com/playlist?list=PLmL13yqb6OxdeOi97EvI8QeO8o-PqeQ0g
- Semtech https://lora-developers.semtech.com/resources/lorawan-academy/
- https://www.silabs.com/documents/public/user-guides/ug103-14-fundamentals-ble.pdf
- Others in the slides

Agenda

- Short range vs long range: general discussion
- Background and recap
  - OSI
  - Radio concepts
- Short range
  - Zigbee, Thread
  - BLE
- Long Range
  - 5G
  - LoRAWAN (if time remains)

Short range vs long range

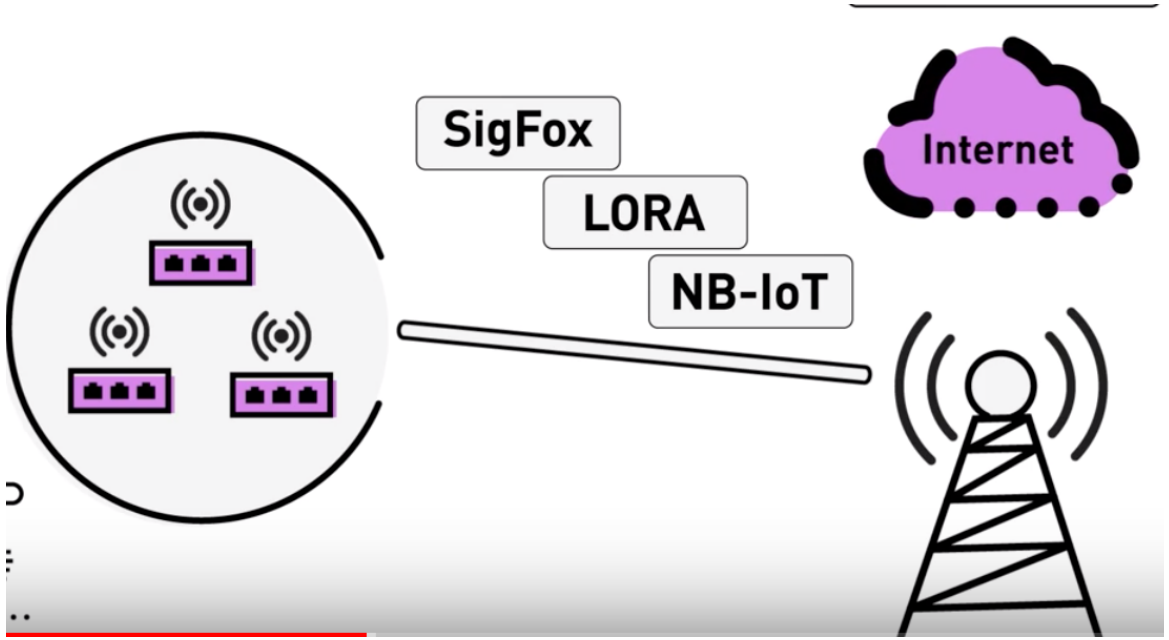
Transport technologies

Ref: www.inov360.com

Short range vs long range

- Many wireless and low power communication technologies have been proposed. They can be mainly classified into two categories:
  - short range and
  - long range
- If we are talking about short range technologies, you might be familiar with some like “Bluetooth Low Energy” or Zigbee. They allow a communication range of 100 to 200 meters while supporting a rate of 100 kilobits per second at 1 Mbps

Long range of some kms

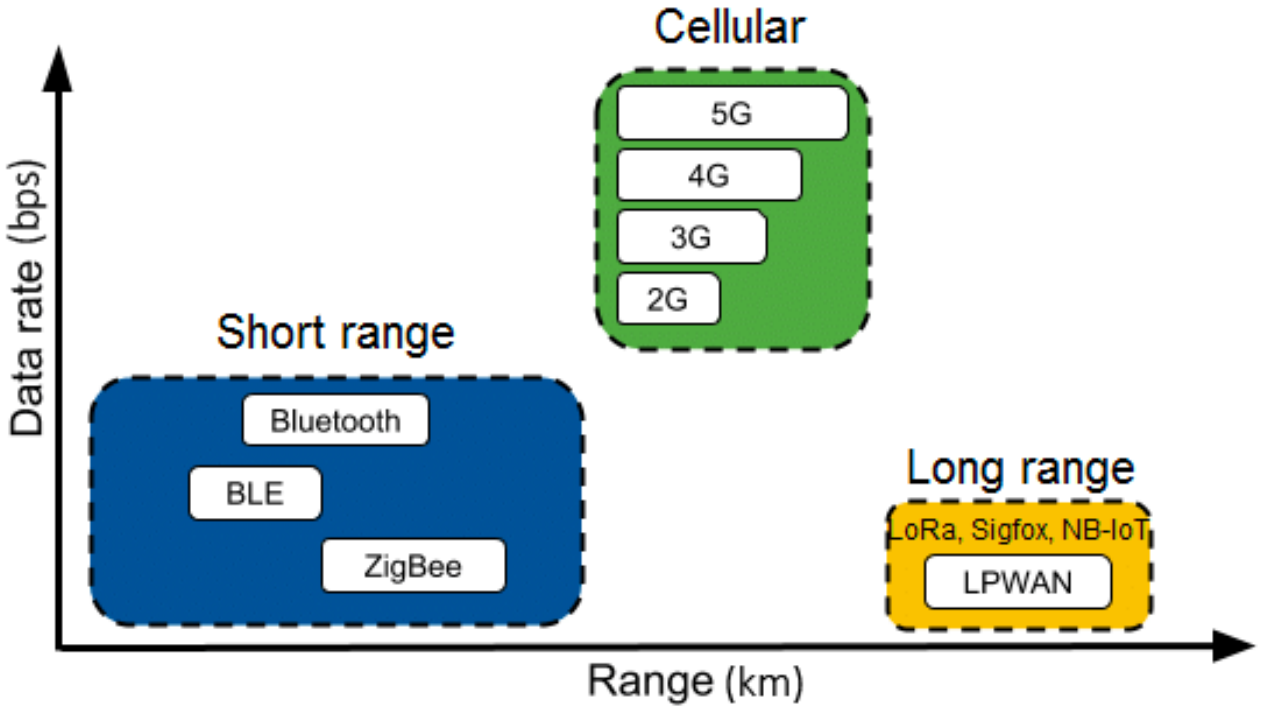


- In some cases, it is better to use long range radio technologies. that simplify the architecture using a single central element. The objects connect to a central gateway using a star topology.
- Several technologies: Sigfox, LoRa or Nb-IoT which is an evolution of cellular networks,
- Range of the order of several kilometers. The speeds are typically low: 1 and 100 kbps

Data rate vs distance

- To choose a technology as a function of application

Ref: https://www.researchgate.net/figure/Range-and-data-rate-of-different-communication-technologies_fig1_332187524



Range comparison

WIRELESS COMMUNICATION COMPARISON

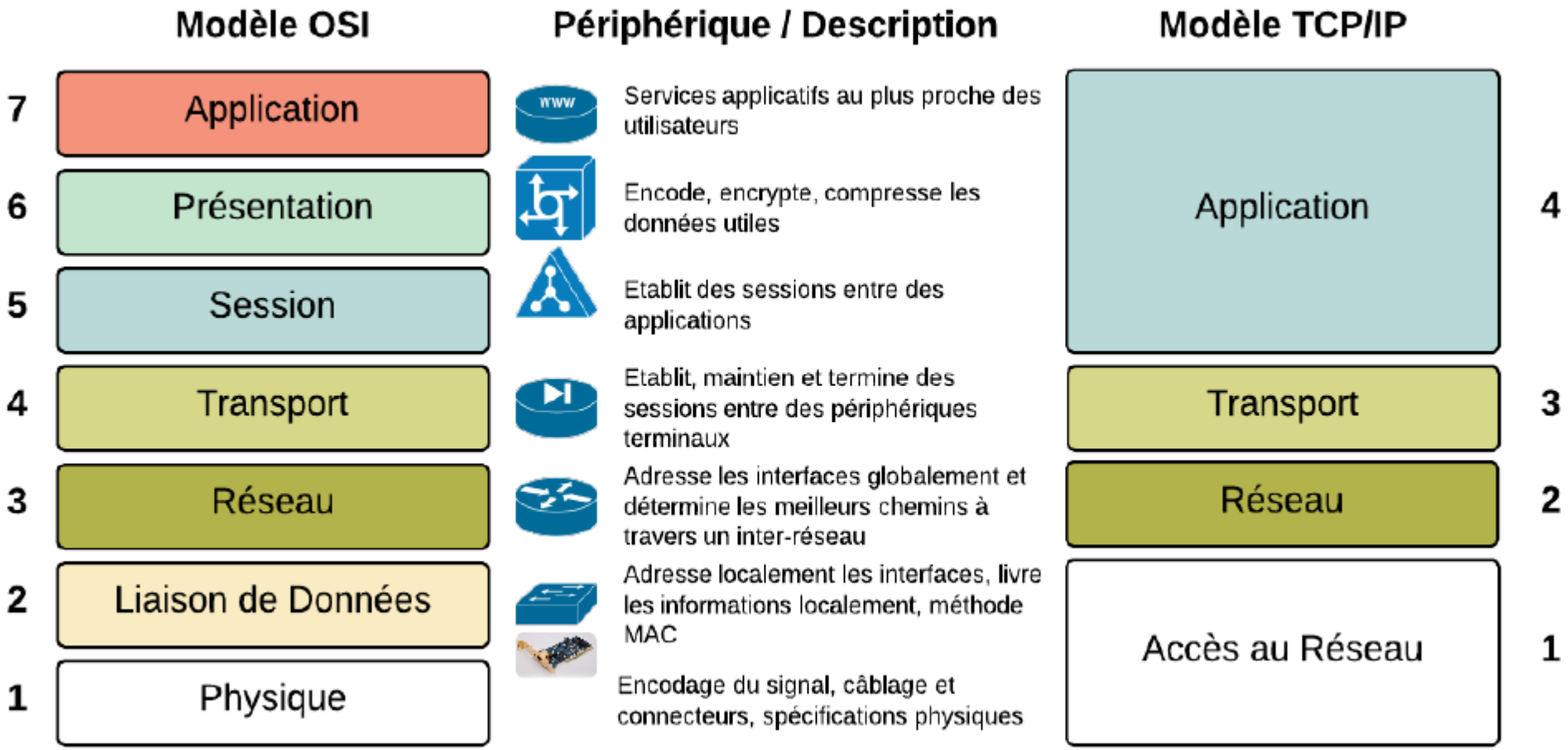
Wireless Technology	Wireless Communication	Range (m)	Tx power (mW)
Bluetooth	Short range	~10	~2.5
WIFI	Short range	~50	~80
3G / 4G	Cellular	~5000	~500
LoRa*	LPWAN	2000-5000 (urban area) 5000-15000 (rural area) > 15000 (direct line of sight)	~20

* Data packages are very small

Ref: Mobilefish

Background

Recall: OSI and TCP/IP

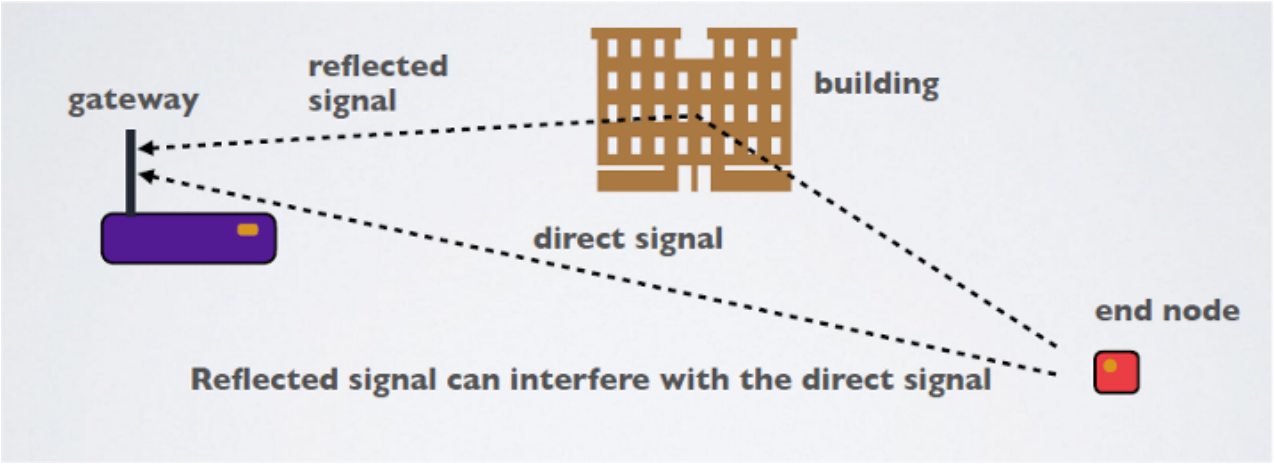


Source: http://cisco.goffinet.org

Radio power

- In energy unit: mW
- And more classic in dBm (decibel / mW)
- Use of the log scale is natural: the attenuation as a function of distance is expressed by a decrease in 1 / r ^ 2
- Complexity of propagation: example of reflections

Ref: Mobilefish



Radio, energy, dissipation

- Transmission chain

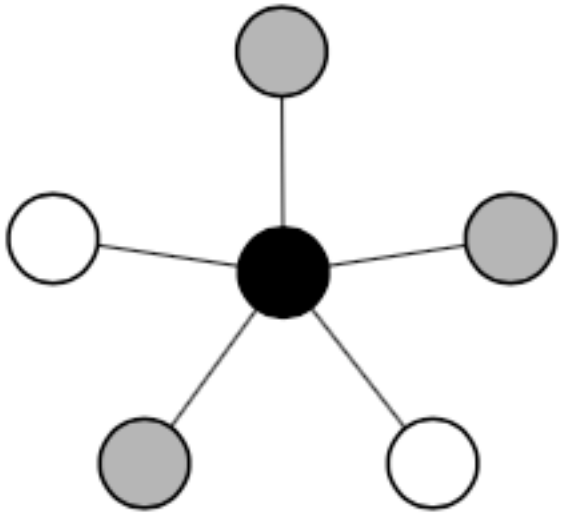
More notions

- RSSI: Received Signal Strength Indication which expresses the reception level allowing to observe a signal (in dBm) always negative value !!
- SNR: Signal to Noise Ratio which expresses the ratio between the background noise and the signal strength

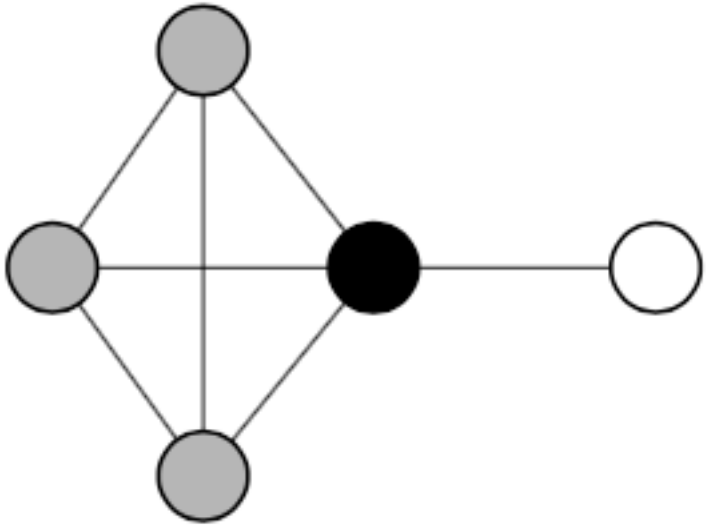
Short Range

Ref: https://hal.archives-ouvertes.fr/hal-02161803/document

Range de 10m, 30m, 100m etc.



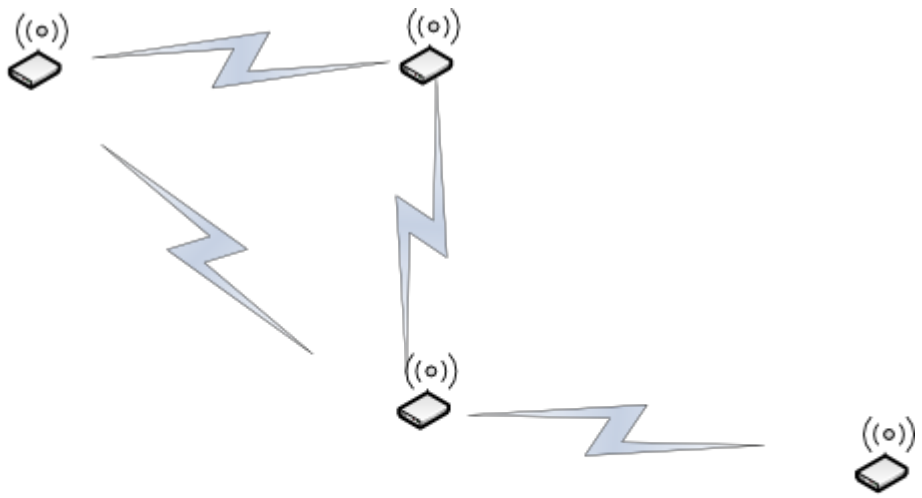
Star Topology



Peer-to-Peer Topology

- Short-range technologies route data either using hop-by-hop routing or by sending the packet directly to a nearby connected gateway. This is possible because these technologies support two types of topologies: mesh and star

Topology



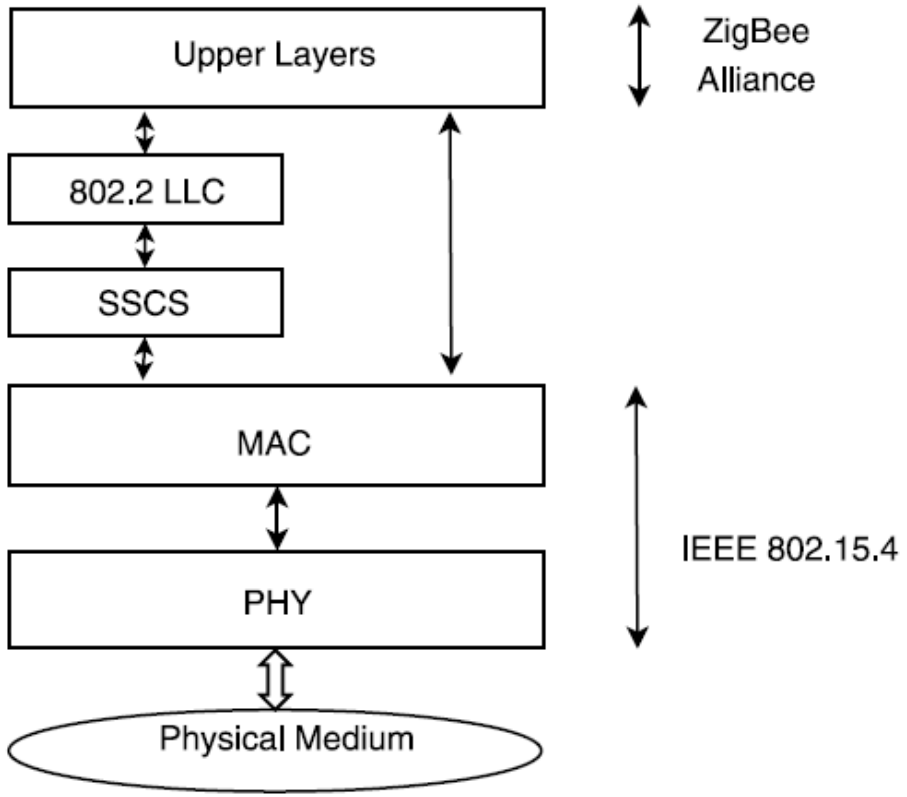
- In the mesh topology, objects connect to each other in an ad hoc fashion and route data through hop-by-hop routing.
- On the other hand, with a star topology, the objects are connected to a central node and they transmit data to that central node, which in turn transmits the data to the destination.
- Short range technologies can be very useful in applications such as home automation, industrial automation, etc.

Examples

- IEEE 802.15.4 /Zigbee
  - 868/915MHz, 2.4GHz
  - 250 kbps
  - 100 m
  - Battery life: Days - years
- Bluetooth Low Energy (BLE)
  - Reduced cost
  - Reduced power consumption
  - Health fitness, Smart devices
- Thread, Z-Wave, ANT, Wavenis, DASH7, ISA100.11a

WSN technologies and standards

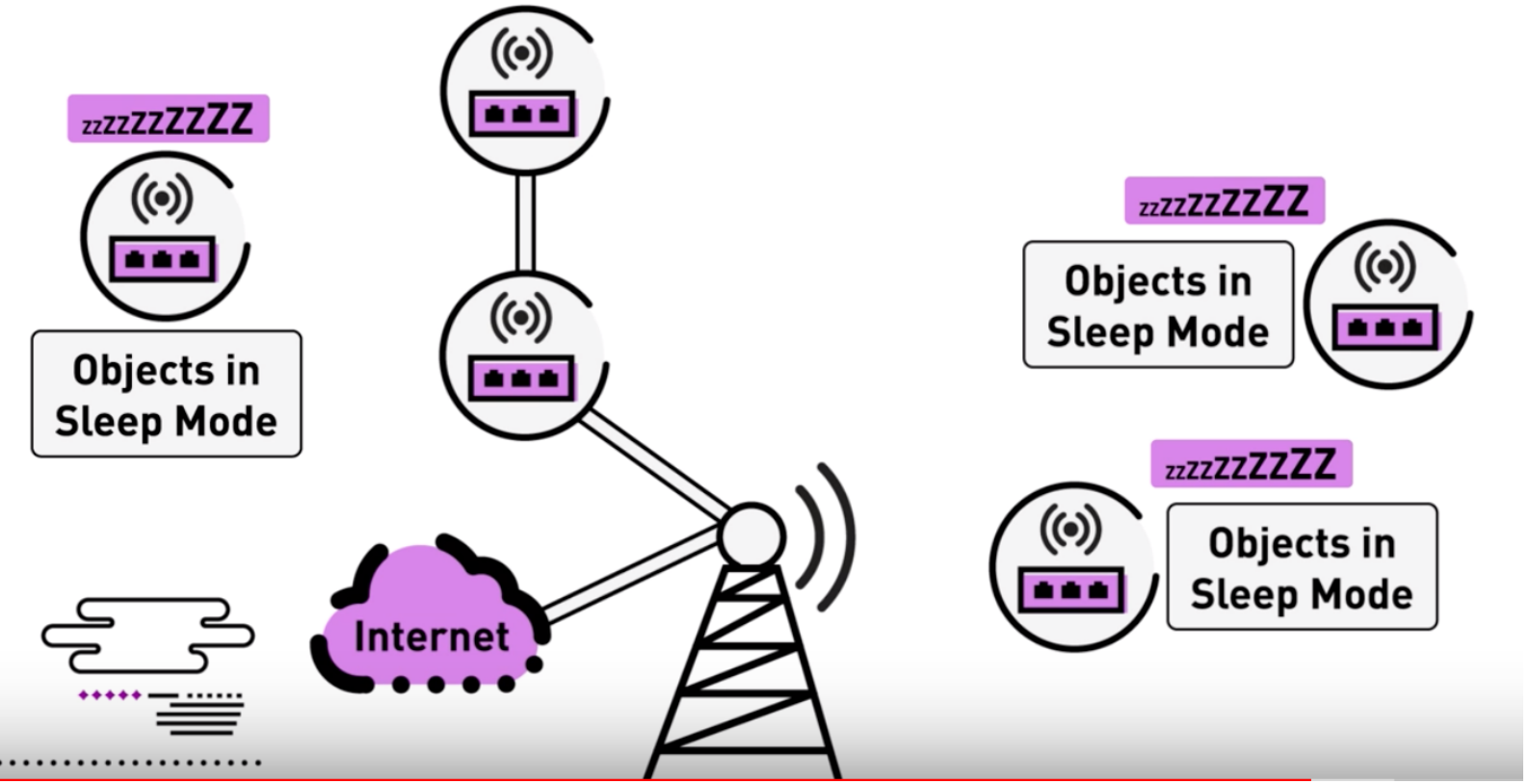
- IEEE normalized MAC and PHY layers
  - IEEE 802.15.4
  - Objective is to design low energy consumption at the cost of short range and low speed



Energy

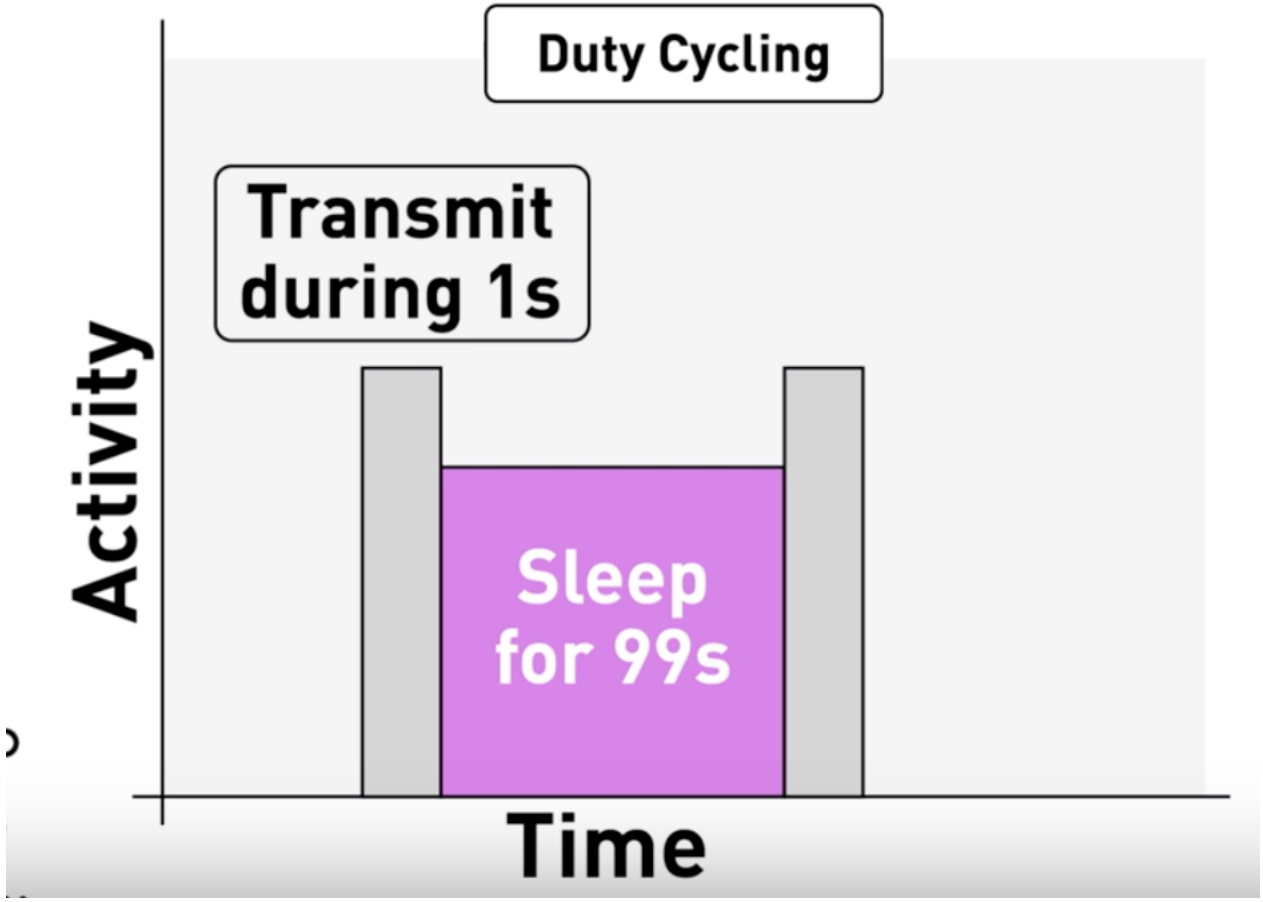
- Communication energy consumption is 220 to 2290 times greater than calculation! (sending a byte vs executing an instruction)
- Transmission or listening both consume energy
- How does IEEE 802.15.4 save energy?

Duty cycle is used in IEEE 802.15.4



- the communication part (transmission and listening) consumes a large percentage of energy. If these are stand-alone, battery-operated objects, it is important to minimize radio use to extend their autonomy. The principle is to let the objects sleep as long as possible.

Duty cycle

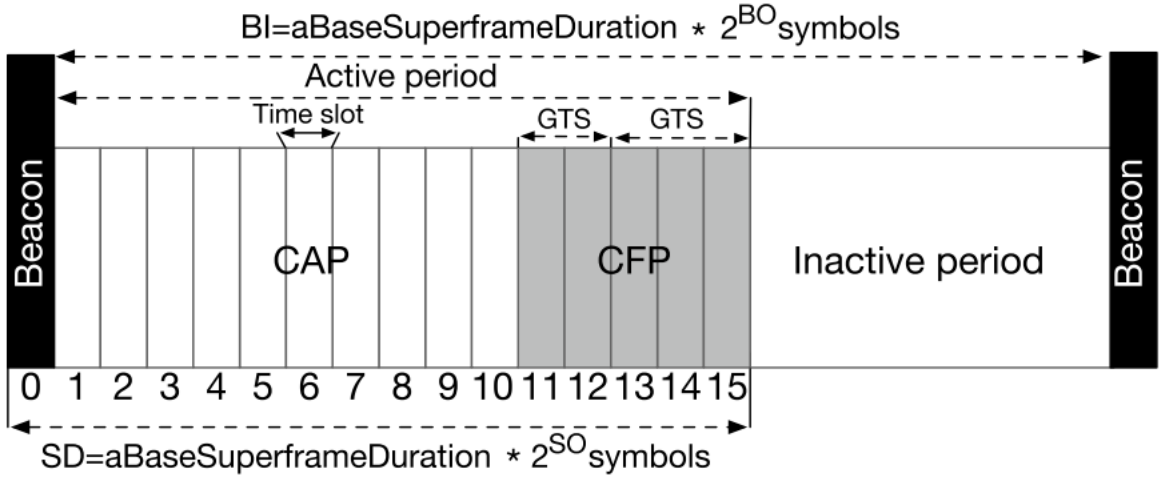

Duty Cycling
Transmit during 1s
Sleep for 99s
Activity
Time

IEEE 802.15.4 Modes and Frame structure

Non beacon mode: every node competes for access

Beacon mode

- Contention Access Period (CAP), Contention Free Period (CFP), duty cycle during inactive period
- Superframe duration includes active and inactive periods
- Parameters
  - Superframe Order (SO) and Beacon Order (BO).
  - coordinator defines the superframe structure using Beacon Interval (BI)
  - Total = Superframe Duration (SD)

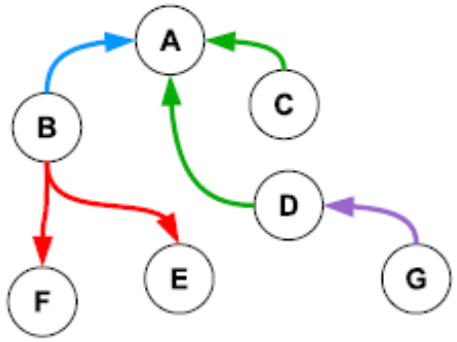


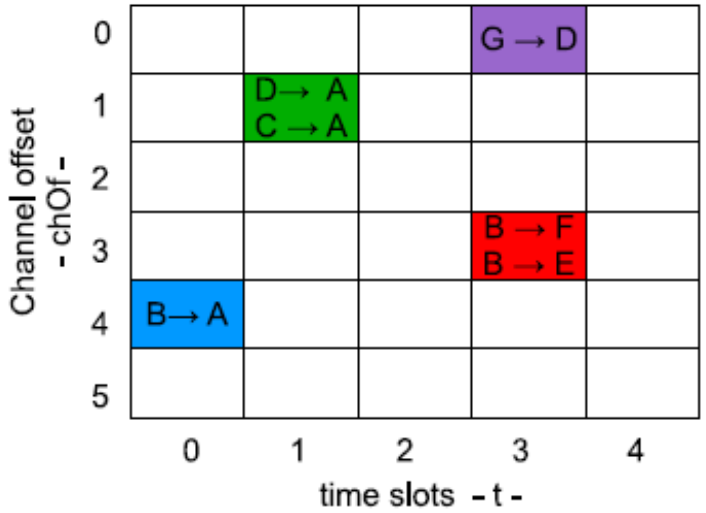
IEEE 802.15.4e

- Another generation of highly reliable and low-power MAC
  - Extension of 802.15.4
- Time Synchronized Channel Hopping (TSCH) and other modes
- Low Energy MAC extension

IEEE 802.15.4e

- Channel Hopping provides robustness against radio interference
- Scheduling impacts throughput, latency and power consumption
- Transmitter and receiver only wake up when truly needed





IEEE 802.15.4e

- Does not define how to build an optimal schedule
- Optimal schedule needs to be designed as a function of
  - Traffic load
  - Energy harvesting
  - Interference
  - Sequence constraints of messaging

Zigbee

Ref: https://hal.archives-ouvertes.fr/hal-02161803/document

Uses IEEE 802.15.4

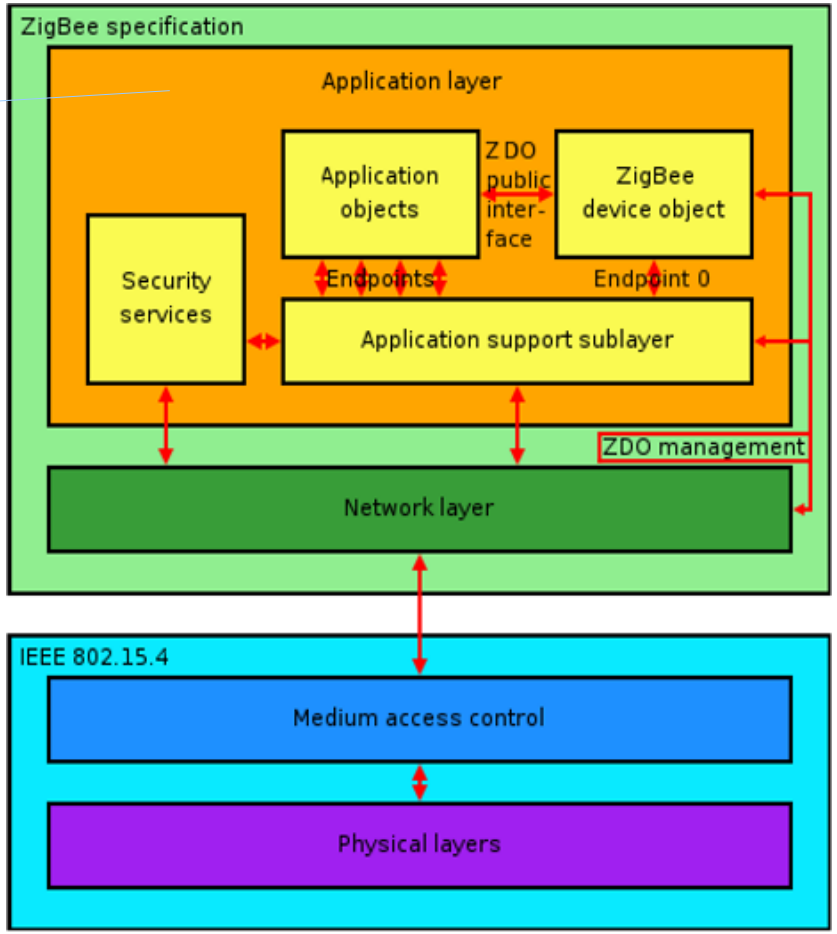
- Application profiles

From wikipedia

L7	APP
L4	TRAN
L3	NET
L2	MAC
L1	PHY

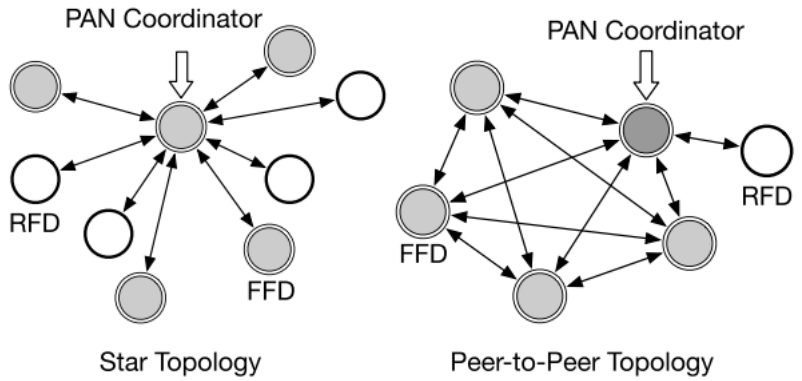
Zigbee

IEEE 802.15



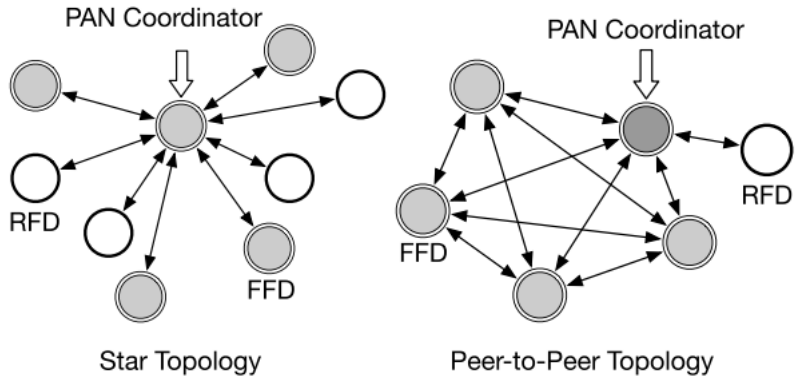
Networking

- Functional entities
  - RFD: Reduce Function Device
  - FFD: Full Function Device
- Star or mesh topology
- Type of physical deices (ZDO : Zigbee Data Object)
  - ZED: zigbee End Device
  - ZR: zigbee Router
  - ZC: zigbee Coordinator



Details on ZigBee Device Classes

- Full function device (FFD)
  - Any topology (tree, star, mesh)
  - Ability to be Router or Network Coordinator
  - Talks to any other device
- Reduced function device (RFD)
  - Topology Limited to star
  - Talks only to an FFD (ZC or ZR)

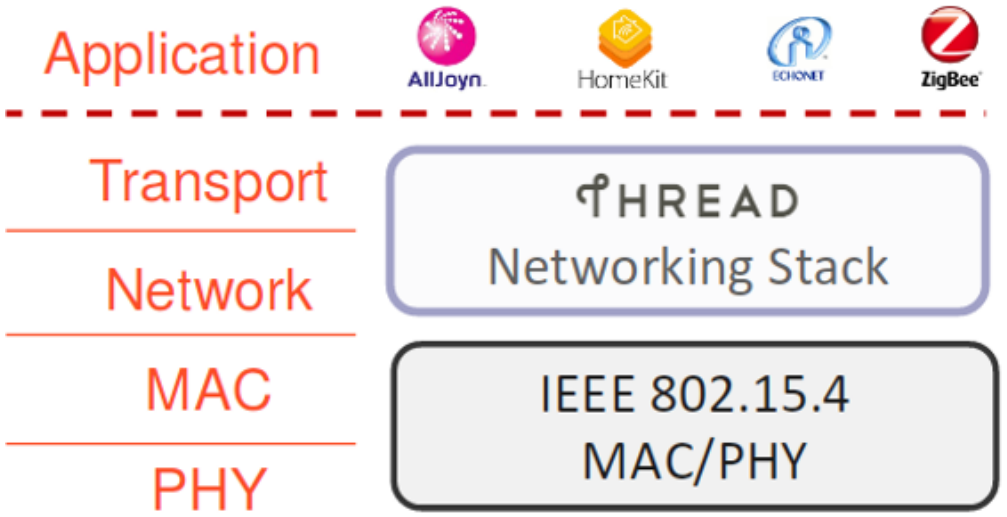


Thread

Thread

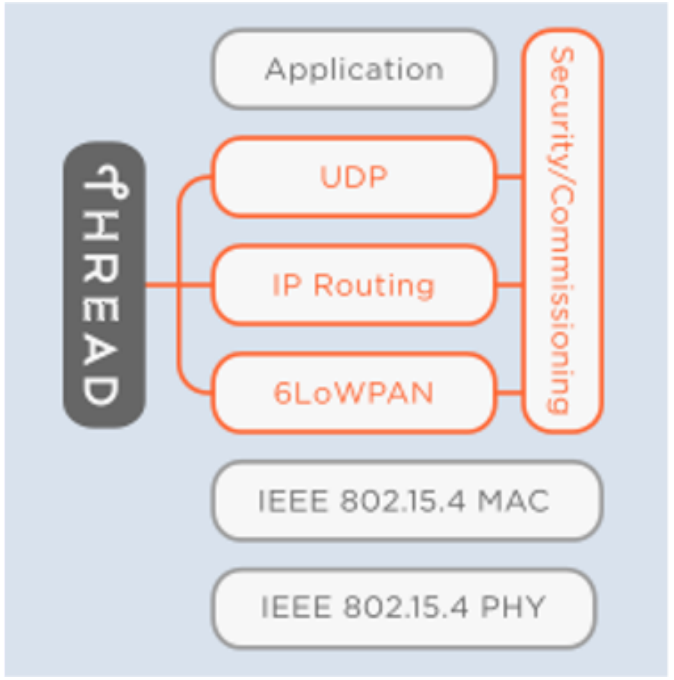
- Thread is an open networking stack, which has received support from well-known organizations such as Google, Samsung, Nest, Freescale, and ARM.
- Natively IP-addressable. Zigbee needs to translate its address to IP for internet, smartphone based Thread authentication and commissioning.
- Ref : https://en.wikipedia.org/wiki/Thread_(network_protocol)
- Official site http://threadgroup.org/
- A complete ecosystem that goes till certification
- Started in 2014, alliance in 2015, opensource in 2016 !!

Layers


Application
AllJoyn
HomeKit
ECHONET
ZigBee
Transport
Network
MAC
PHY
THREAD
Networking Stack
IEEE 802.15.4
MAC/PHY

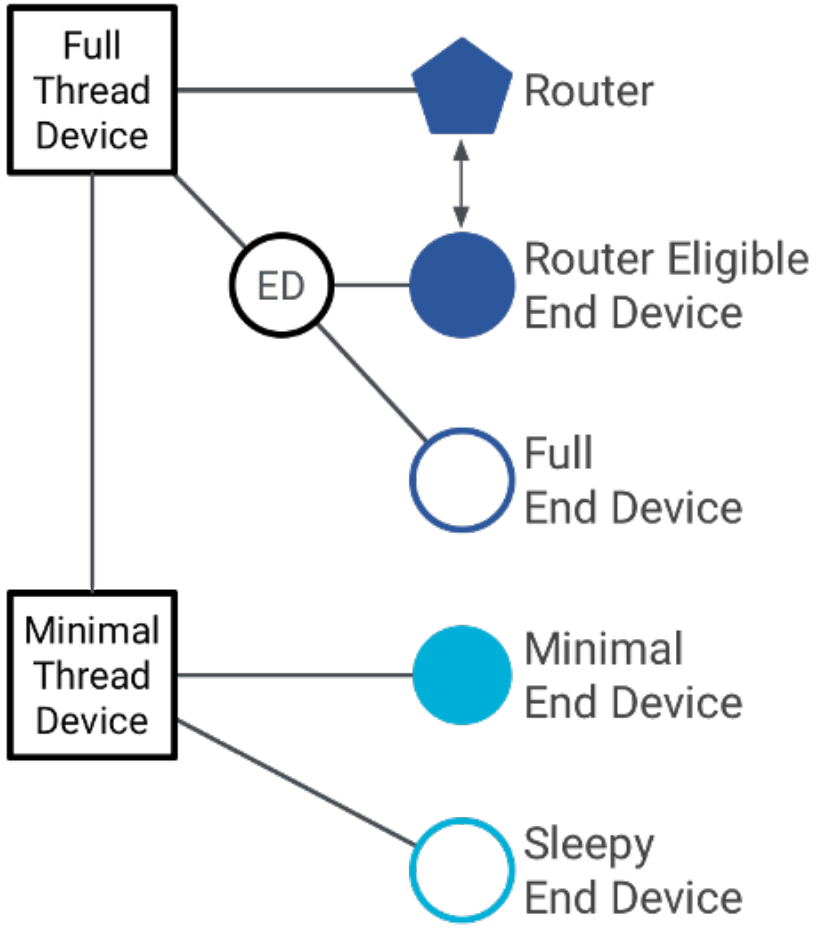
Radio

- Radio in the ISM band (2.4Ghz): no license purchase
- Low power compatible radio transmission: battery operation and long duration
- Mesh network up to 250 devices
- Encrypted messages and secure network
- IP type addressing
- Simple installation (using smartphone!)



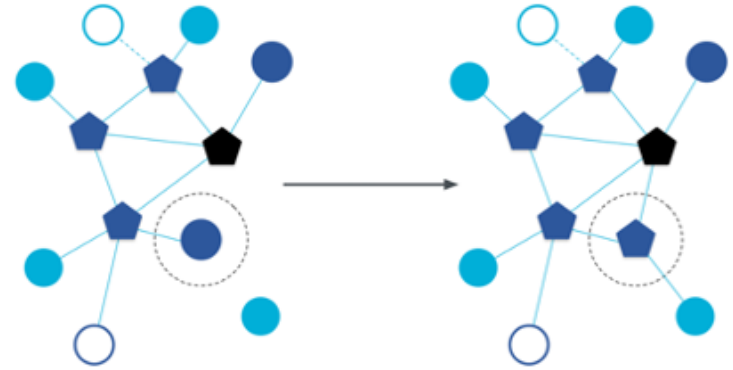
Network

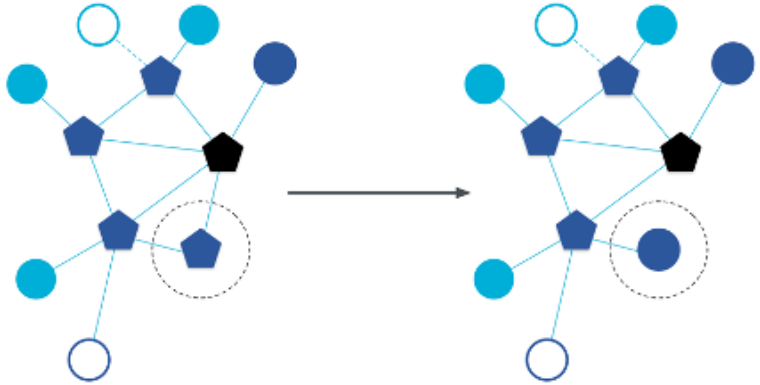
- The nodes have different states
  - Full, Minimal
- Different roles
  - Router, End Device (ED)
- Network is dynamic
  - Change of roles (Eligible) depending on energy state



Dynamic mesh network

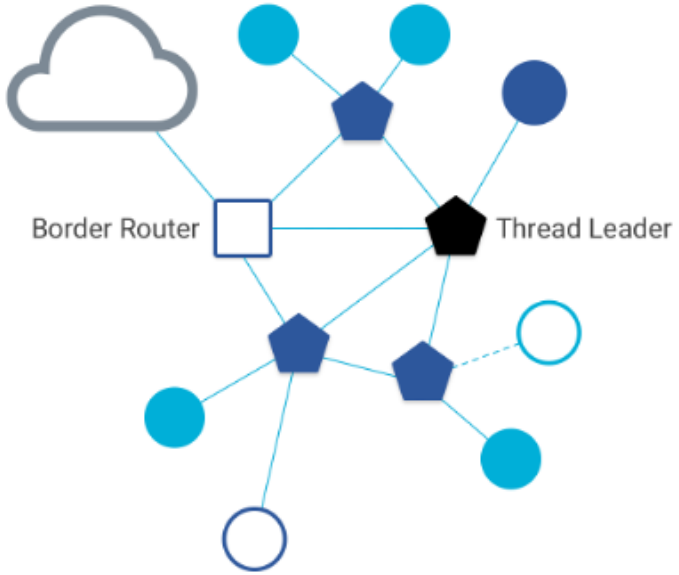
- Router, but not always!
  - Software complexity
  - But gain in energy

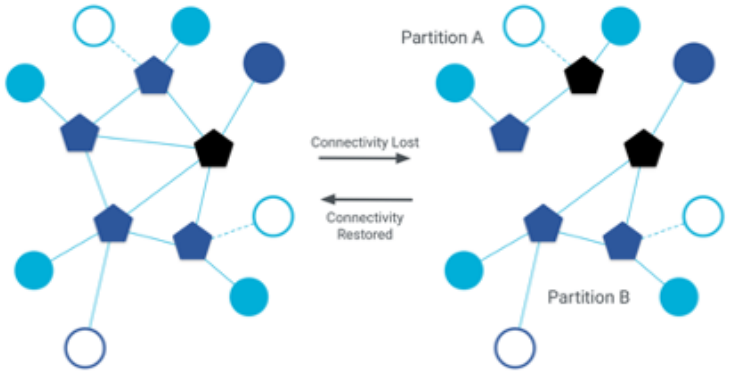




Dynamic mesh network

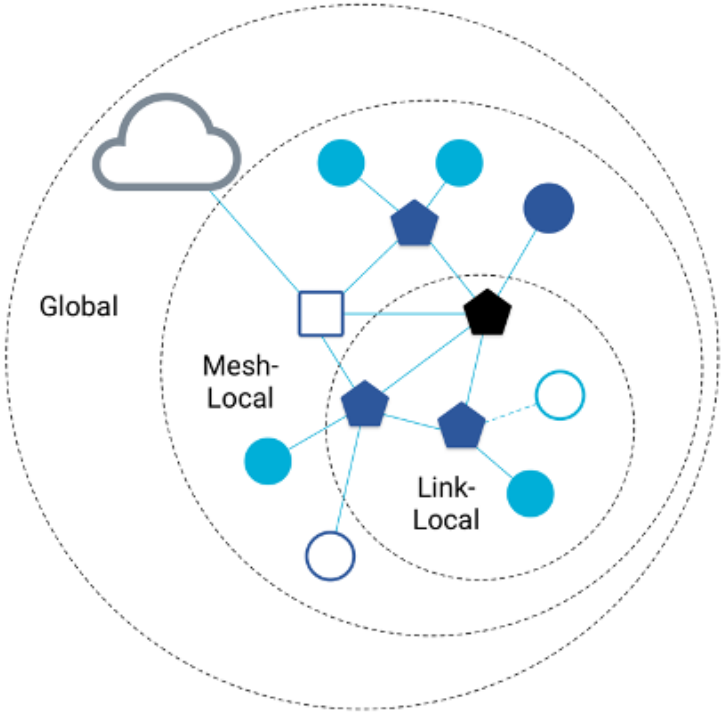
- Border and leader!
  - A network can have many border routers





IPv6 addresses

- Link-Local have prefixes of fe80::/16
- Mesh-Local have prefixes of fd00::/8
- unicast, multicast, anycast



BlueTooth

https://fr.wikipedia.org/wiki/Bluetooth

https://learn.sparkfun.com/tutorials/bluetooth-basics/all

https://www.silabs.com/documents/public/user-guides/ug103-14-fundamentals-ble.pdf

https://hal.archives-ouvertes.fr/hal-02161803/document

History

- Beginning in 1994… Ericsson… then an alliance to manage this standard, the SIG: Bluetooth Special Interest Group, see the site at https://www.bluetooth.com/
- Permanent evolution
  - Bluetooth v1.0 and v1.0B
  - Bluetooth v1.1, standardized in 2002 under the name IEEE 802.15.1-2002
  - Bluetooth v1.2, standardized in 2005 under the name IEEE 802.15.1-2005
  - Bluetooth v2.0 + EDR, in 2003 and v2.1 + EDR, in 2007
  - Bluetooth v3.0 + HS, released in 2009;
  - Bluetooth v4.0 + LE, released in 2010
  - Bluetooth v4.1, in 2013 followed by 4.2, end of 2014
  - Bluetooth v5, late 2016; and Bluetooth Mesh, an option made public in July 2017 which only applies to the BLE version.
- 2 major categories:
  - First, Bluetooth **Basic Rate** and **Enhanced Data Rate(BR/EDR)** refers to the earlier versions of Bluetooth mainly designed for file transmission and audio streaming.
  - Second, **BLE** refers to the recent versions of Bluetooth targeting low-power consumption for IoT applications

Radio

- IEEE 802.15.1
- ISM 2.4GHz: from 2.402 to 2.480
- Gaussian Frequency Shift Keying (GFSK) modulation
- 3 classes (according to power)

Class	Power	Range
1	100 mW (20 dbm)	100m
2	2.5 mW (4 dbm)	20m
3	1 mW (0 dbm)	some m

- Difference between BT classic and BLE channels

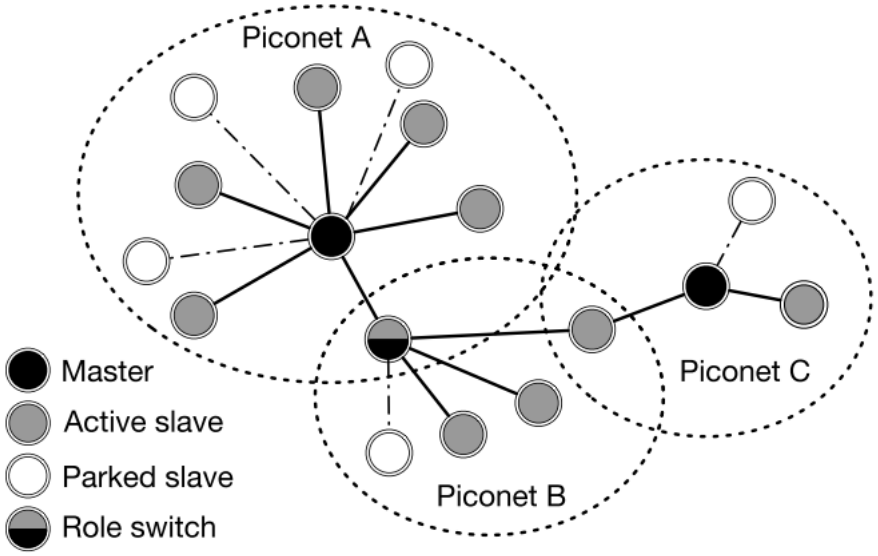
BT EDR	BLE
79 channels with 1 MHz spacing	40 channels with 2 MHz spacing (3 advertising channels /37 data channels)

Ranges

- https://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range

	BT v2.1	BT 4 LE	BT 5 LE
Range	100 m	100 m	400 m
Data Rate	2.1 Mb/s	305 kbit/s	1360 kbit/s
Topologies	scatternet	mesh	mesh

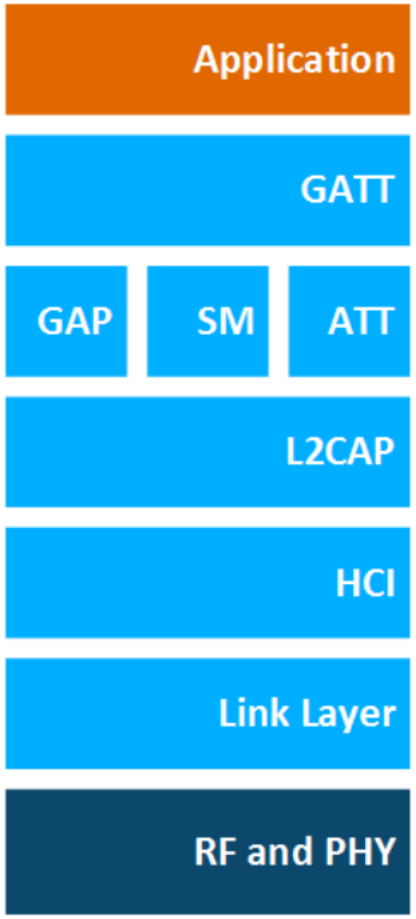
General notions



General notions

- A major disadvantage of BR/EDR is high power consumption.
  - continuous polling of the slave nodes by the master node even in the absence of data to transmit.
  - scanning of a large number of channels (32 channels) for Device Discovery.
- BLE
  - link layer, PHY, packet formats redesigned.
  - capable of either only a transmitter or a receiver.
  - only 3 advertisement channels as compared to 32 in BR/EDR
  - simplified link layer and packet formats

BLE architecture



Controller layers:

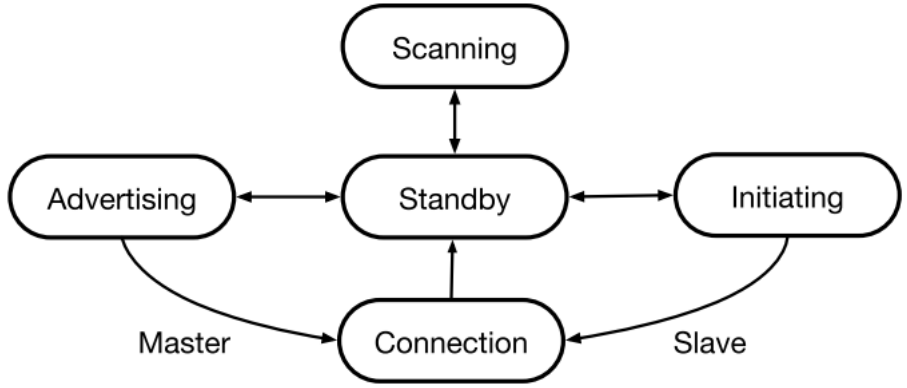
- Physical layer: Controls radio transmission/receiving.
- Link Layer: packet structure, state machine and radio control, encryption.

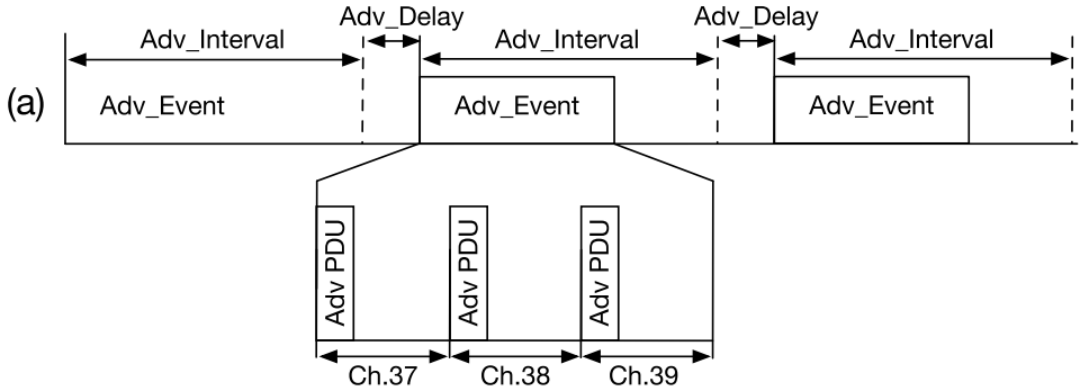
Rest higher layers are called host layers:

- Host-to-Controller interface (HCI) standardizes controller-host communication
- L2CAP: Logical Link Control and Adaptation Protocol: protocol multiplexer, handles segmentation, reassembly of packets, logical channels
- ATT: Attribute Protocol provides means to transmit data between Bluetooth low energy devices
  - Procedures for read, write, indicate and notify attribute values over that connection.
- GATT: Generic Attribute Profile: used to group individual attributes into logical services
  - for example the Heart Rate Service, which exposes the operation of a heart rate sensor.
  - information about the attributes i.e. how they can be accessed and what security level is needed
- GAP: Generic Access Profile. To advertise themselves or other devices, make device discovery, open and manage connections and broadcast data.
- SM: Security Manager. bonding devices, encrypting and decrypting data, device privacy.

Link Layer (state machine)

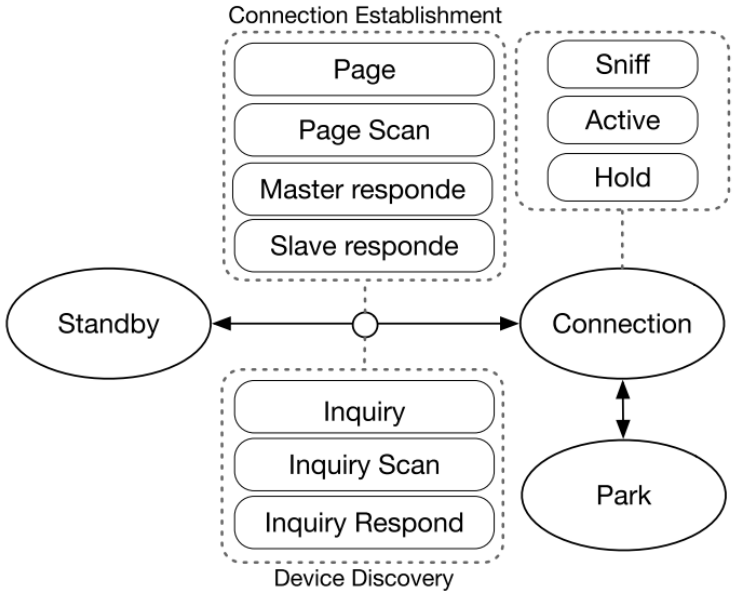
- Standby: initial default state to save power with no send or recv
- Advertising: first step for any BLE connection.
  - advertisement channels broadcast PDUs.
    - non-connectable advertising
    - connectable advertising
    - discoverable advertising
    - directed advertising,
    - scan request, scan response,
    - or connect request
  - may result in communication establish-ment or merely broadcasting data.





Link Layer (state machine) …

- Scanning state has 2 parts:
  - passive scan, the receiver only listens and does not respond.
  - active scan, the receiver may respond to get more info
- Initiating: on reception of advertisement it responds by initiating packets.
- Connection: if need to switch to data channels and exchange information.
  - advertiser becomes the master node, and the initiater becomes a slave node.



Security

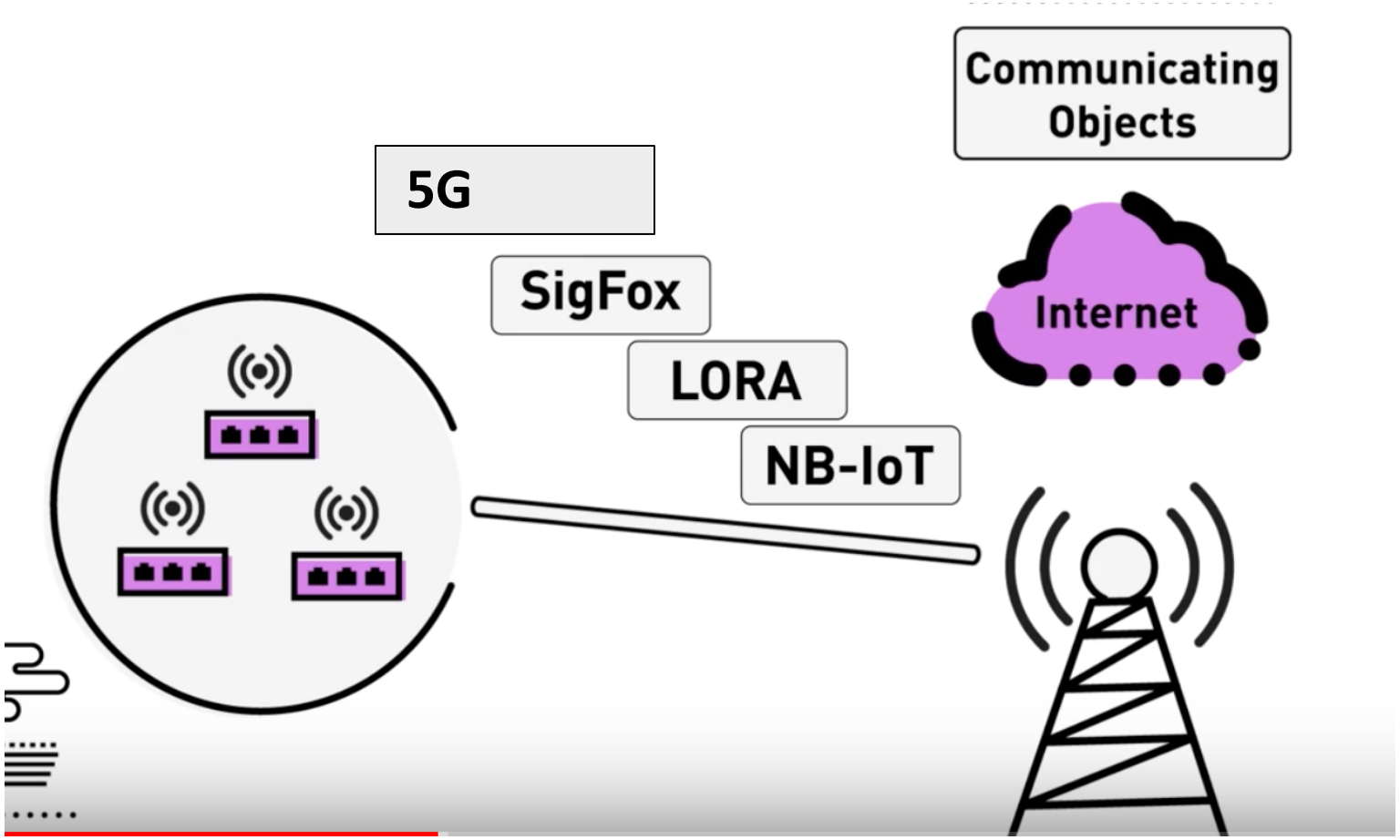
- Pairing: the process for creating shared secret keys
- Bonding: storing the keys created during pairing so they can be used later
- Device authentication: verification of stored keys
- Encryption: data confidentiality
- Message integrity: protection against data alteration

Other features

- A Bluetooth beacon is equipped with BLE
  - A simple one-way communication channel.
  - Beacon has 31 Bytes, enough for short messages, service advertisements
- Very recent: the emergence of geolocation capability in theory to the nearest cm.
  - From bluetooth 5.0 onwards

Long Range

Long Range



5G

What does 5G bring for IoT?

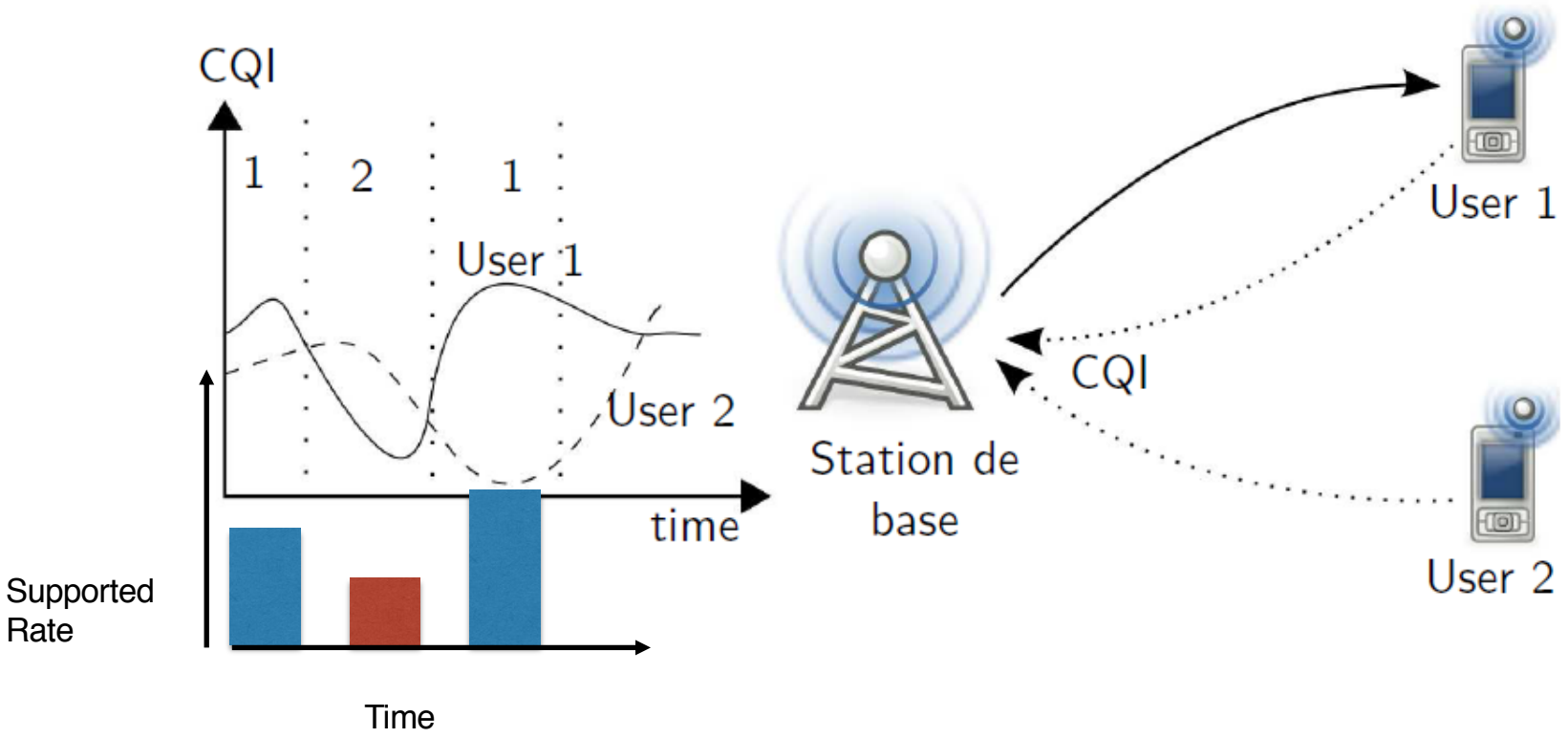
- Private 5G networks
- Transportation of other network technologies: ethernet, CAN
- Enhanced ultra-reliable low latency communication (eURLLC) for TSN (Time sensitive network)
- Scalability with the help of virtualisation and disaggregation
- Low latency with the help of Edge computing

Radio

- New Radio
  - Frequency Range 1 (FR1), including sub-6 GHz frequency bands
  - Frequency Range 2 (FR2), including frequency bands in the mmWave range (24–100GHz)
    - Rapid attenuation of FR2, more reflections thus suitable for short range communication

BACKGROUND

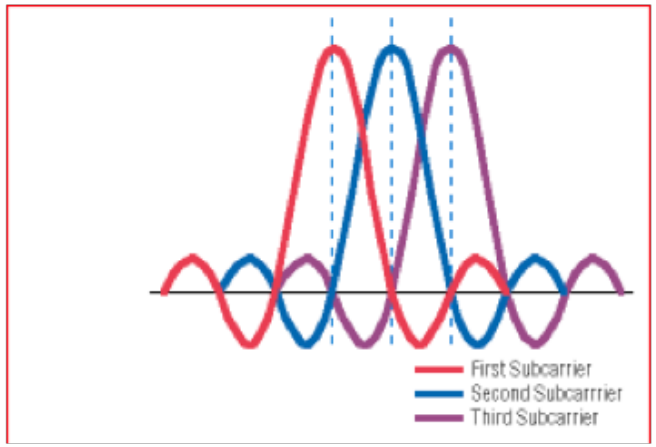
3.5G: for every **time slot**, TTI (2ms), the scheduler gives the channel to the user wit

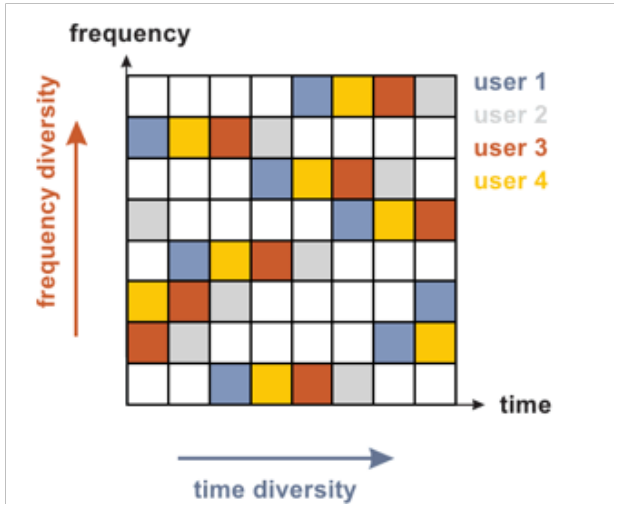


BACKGROUND: OFDMA (USED IN LTE, NB-IOT, 5G)

OFDMA (Orthogonal Frequency Division Multiple Access) :

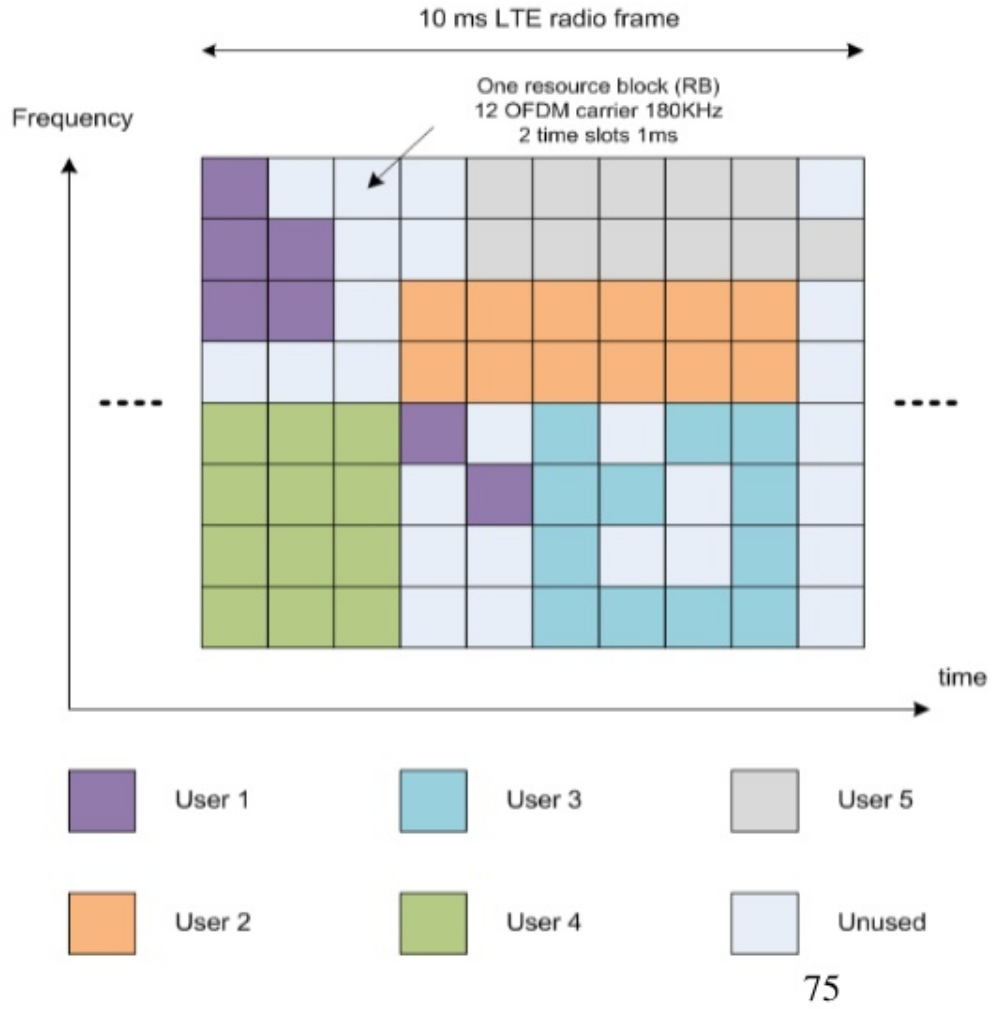
- multiplexages en fréquence et temporel





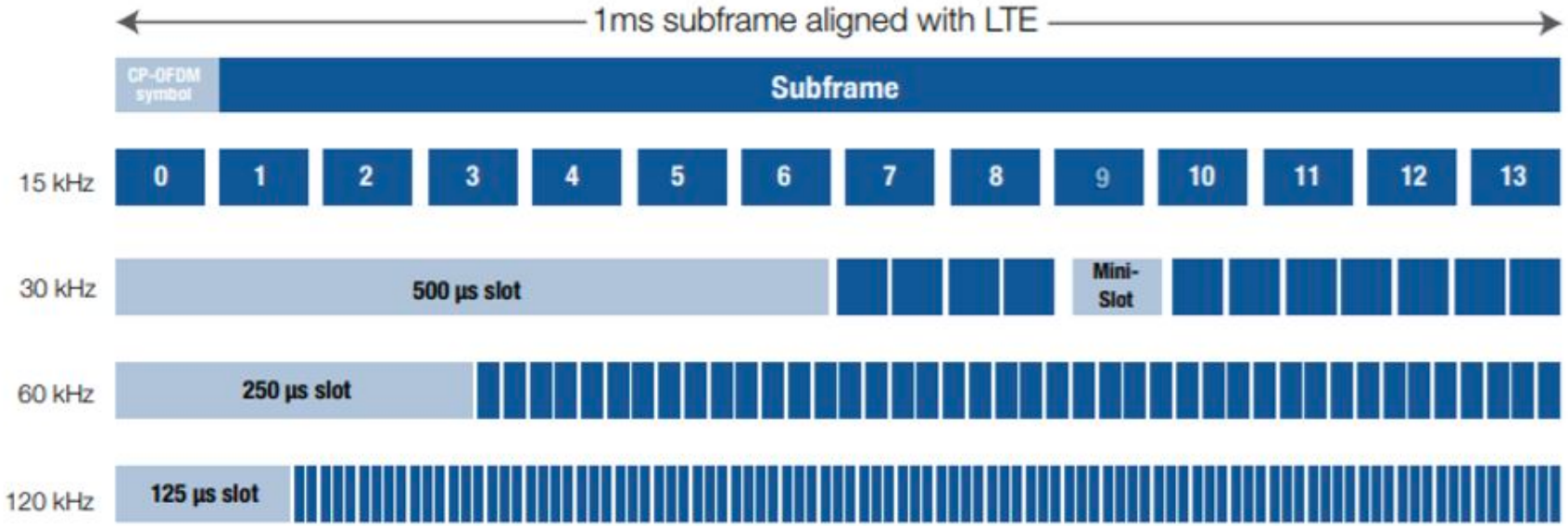
BACKGROUND: 4G (LTE-ADVANCED)

- Minimum allocateable resource in LTE is Resource Block pair
- Resource block pair is 12 subcarriers wide in frequency domain and lasts for two time slots (1ms)
- Depending on the length of cyclic prefix RB pair may have 14 or 12 OFDM symbols
- PHY channels consist of certain number of allocated RB pairs
- Overhead channels are typically in a predetermined location in time frequency domain
- Allocation of the radio block is done by scheduler at eNode B



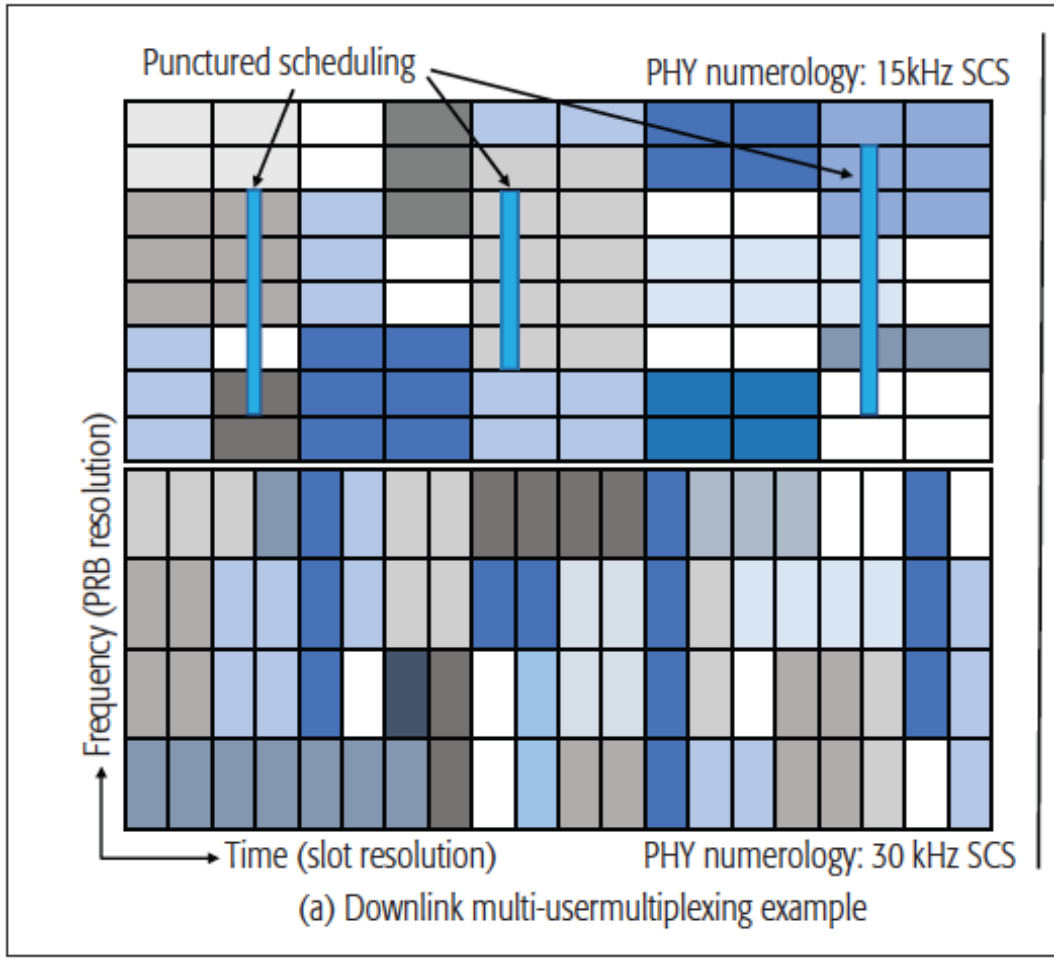
NUMEROLOGY

- Many more parameters to consider
- **PHY numerology**: different subcarrier spacing (SCS) instead of fixed (15 (LTE), 30, 60, 120 and 240 KHz).
  - Slot length gets shorter as subcarrier spacing gets wider because a symbol with higher frequency will take less time



5G

- In the example here a carrier is configured to allow frequency domain multiplexing of two different PHY numerologies, 15 kHz (upper part) and 30 kHz (lower part)



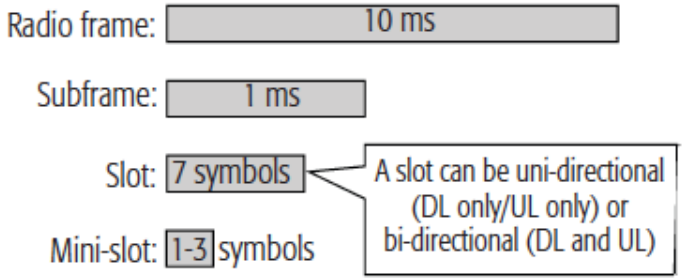
(a) Downlink multi-usermultiplexing example

5G

- Mini-slots of 1-3 OFDM symbols are defined. The smallest time-domain scheduling resolution for the MAC scheduler is a **mini-slot**

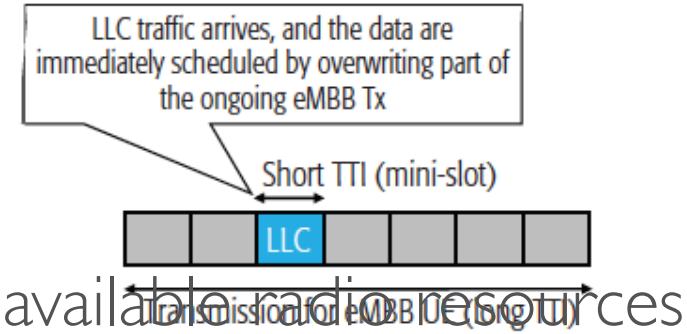
- dynamic scheduling with different transmission time interval (TTI) sizes is supported. (**sometimes in micro seconds**)

- In the frequency domain, the minimum scheduling resolution is one physical resource block of 12 subcarriers, corresponding to 180 kHz for 15 kHz SCS, 360 kHz for 30 kHz, and so forth



5G

Puncture scheduling

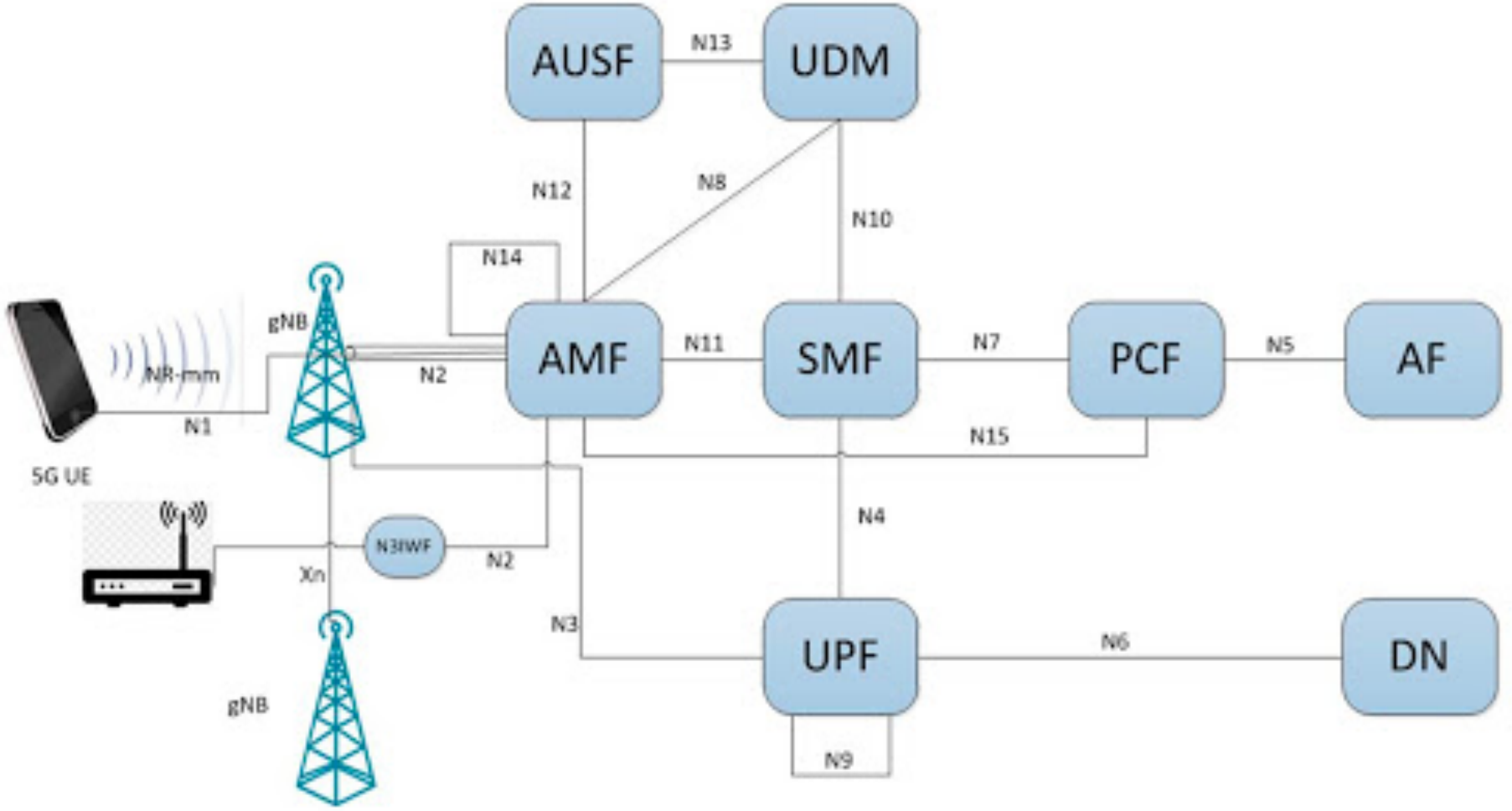


- Normal traffic is scheduled on all the available radio resources (whenever there is sufficient offered traffic).
- Once an LLC (Low Latency Communication) packet arrives at the gNB (5G base station),
  - the MAC scheduler immediately transmits it to the designated terminal by **overwriting** part of an ongoing scheduled transmission, using minislot transmission.

Reference : Pedersen, K. I., Pocovi, G., Steiner, J., & Maeder, A. (2018). Agile 5G Scheduler for Improved E2E Performance and Flexibility for Different Network Implementations. I E E E Communications Magazine, 56(3), 210-217.

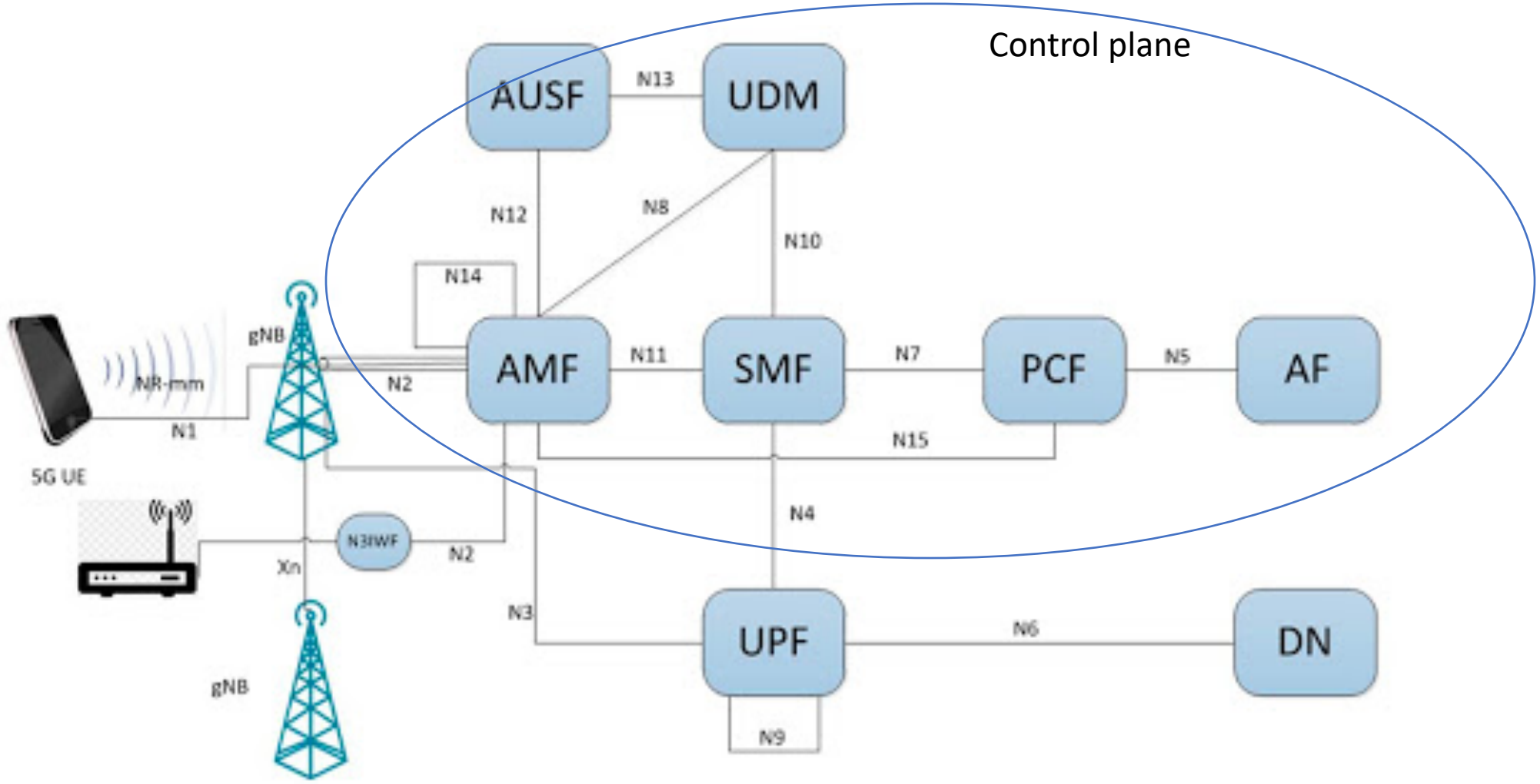
ARCHITECTURE

5G standalone : core and radio access network (RAN)
5G non standalone: only RAN

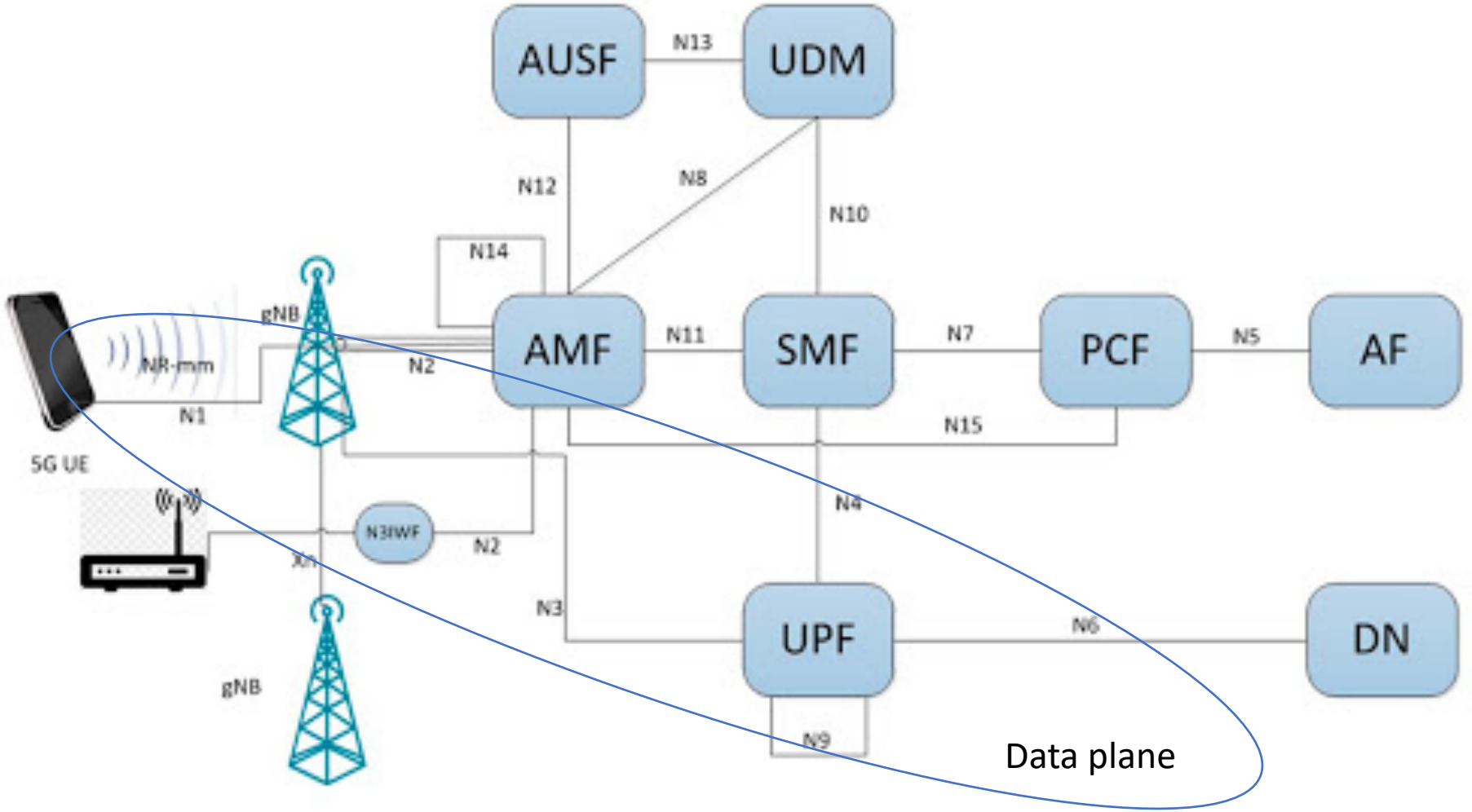


Ref: http://5gblogs.com/5g-network-architecture/

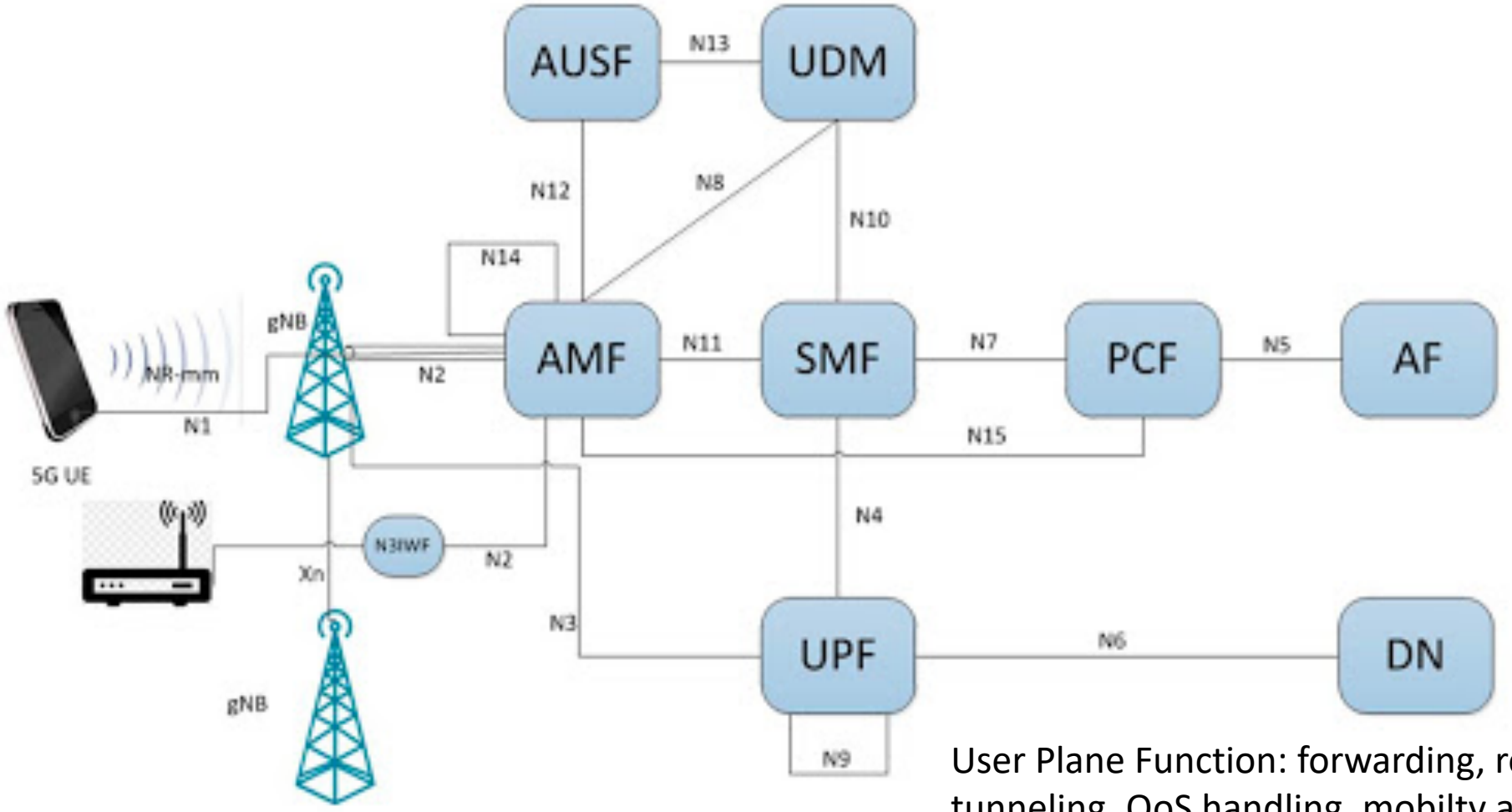
ARCHITECTURE



ARCHITECTURE

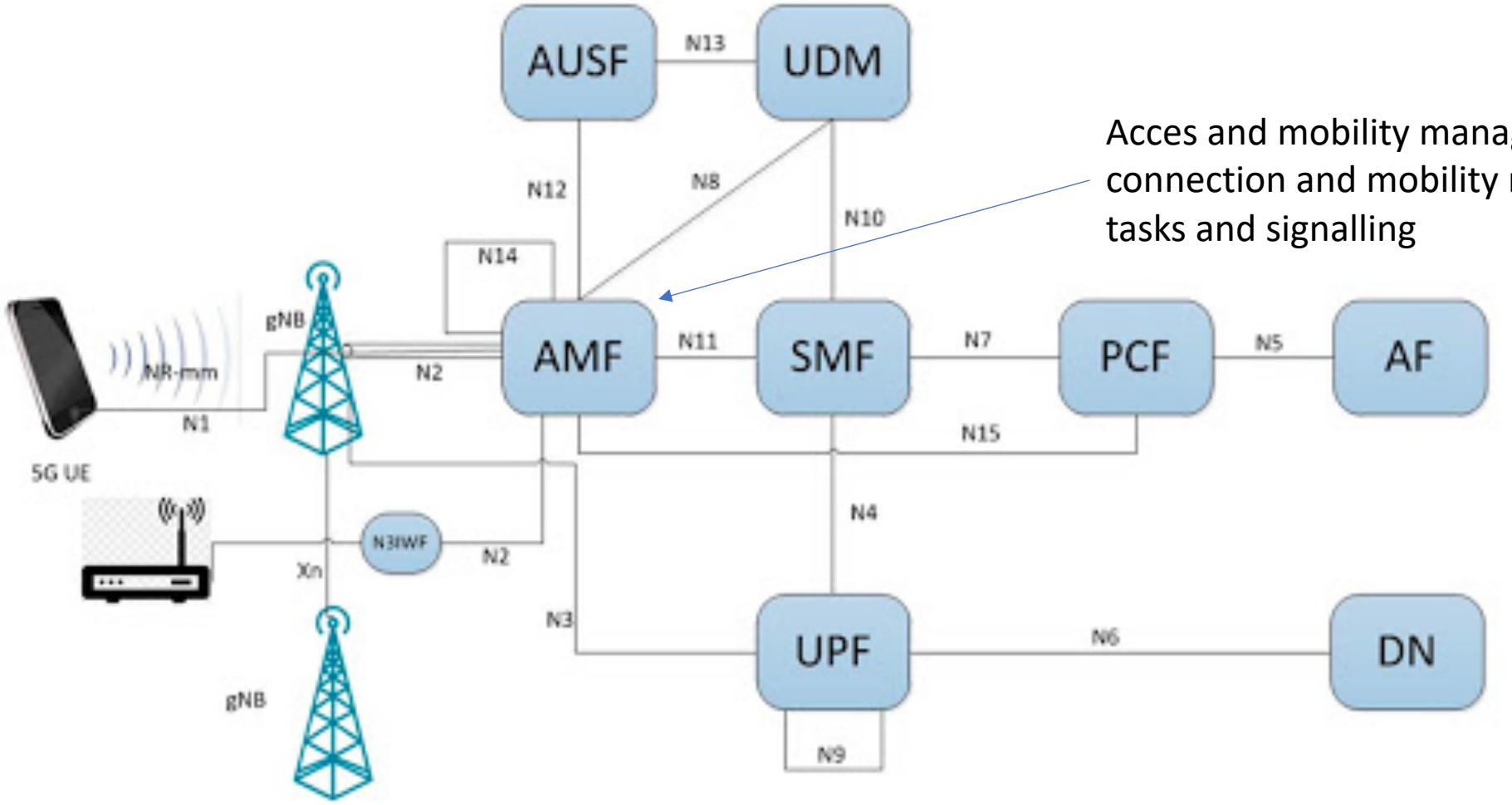


ARCHITECTURE



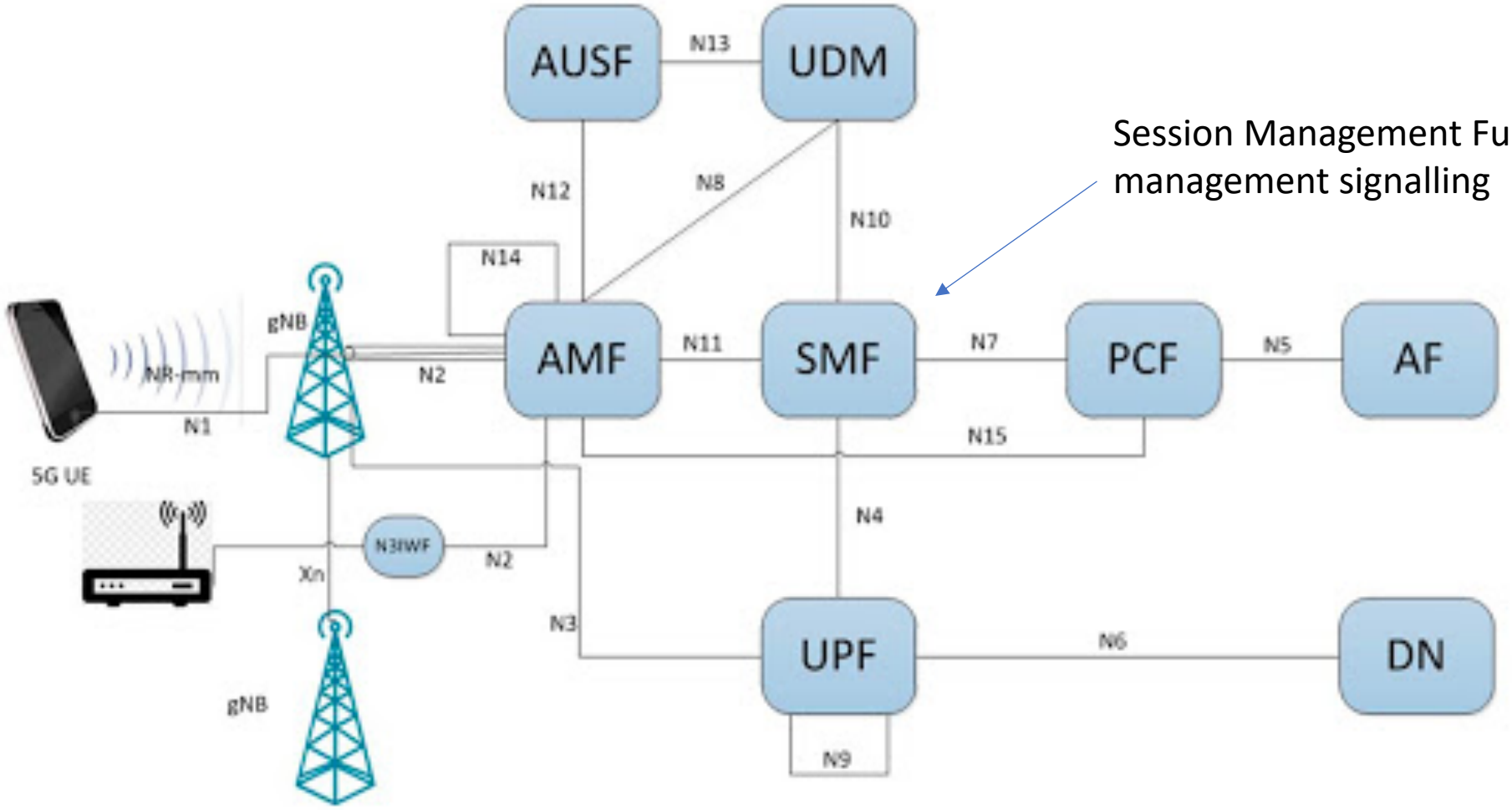
User Plane Function: forwarding, routingn tunneling, QoS handling, mobilty anchor, etc.

ARCHITECTURE



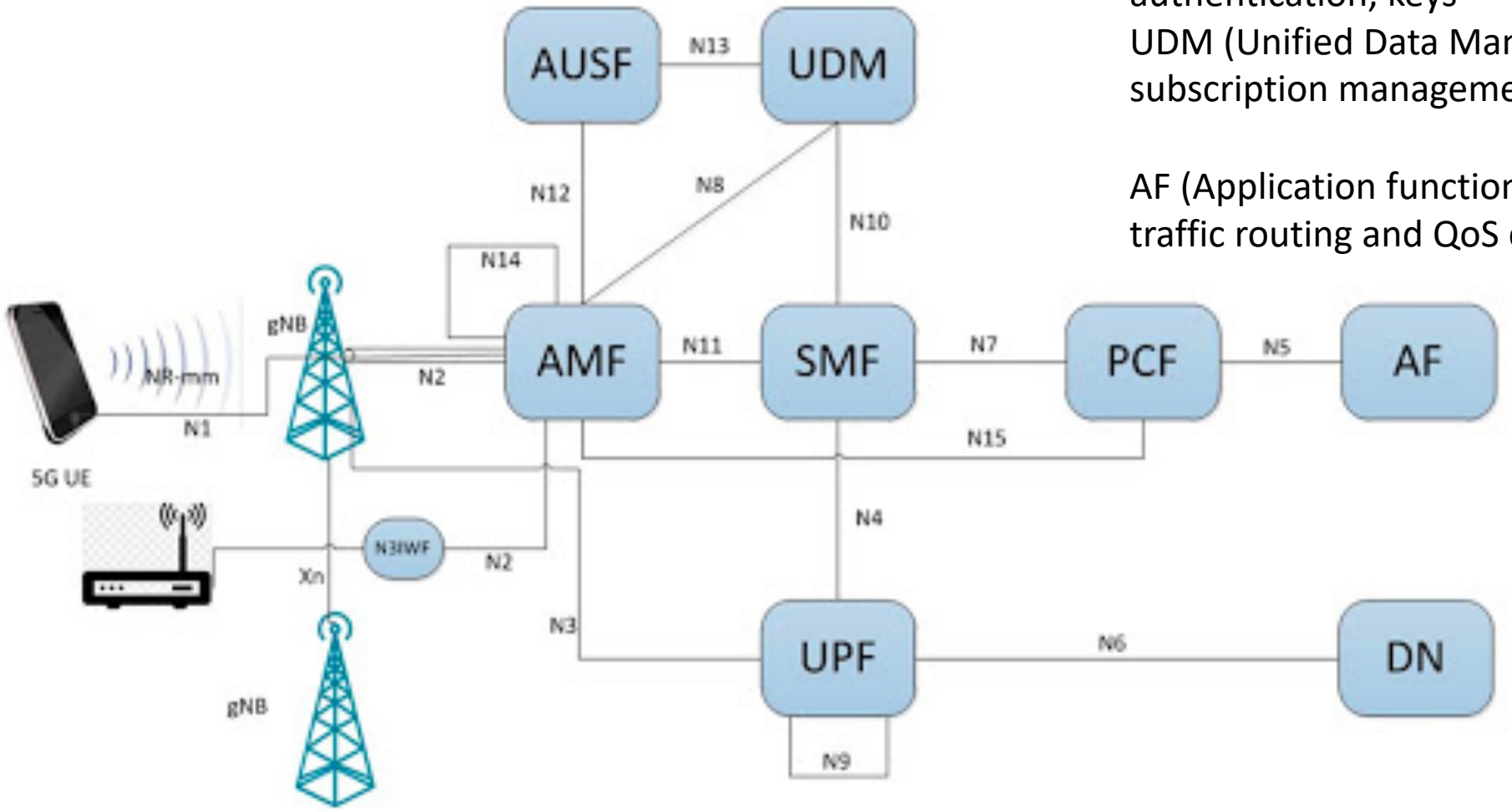
Acces and mobility management function: connection and mobility management tasks and signalling

ARCHITECTURE



Session Management Function: session management signalling

ARCHITECTURE



PCF (Policy Control Function): for example to install QoS rules implement charging policies etc.

AUSF (Authentication Server Function): authentication, keys
UDM (Unified Data Management): identification, subscription management

AF (Application functions): application related traffic routing and QoS configuration

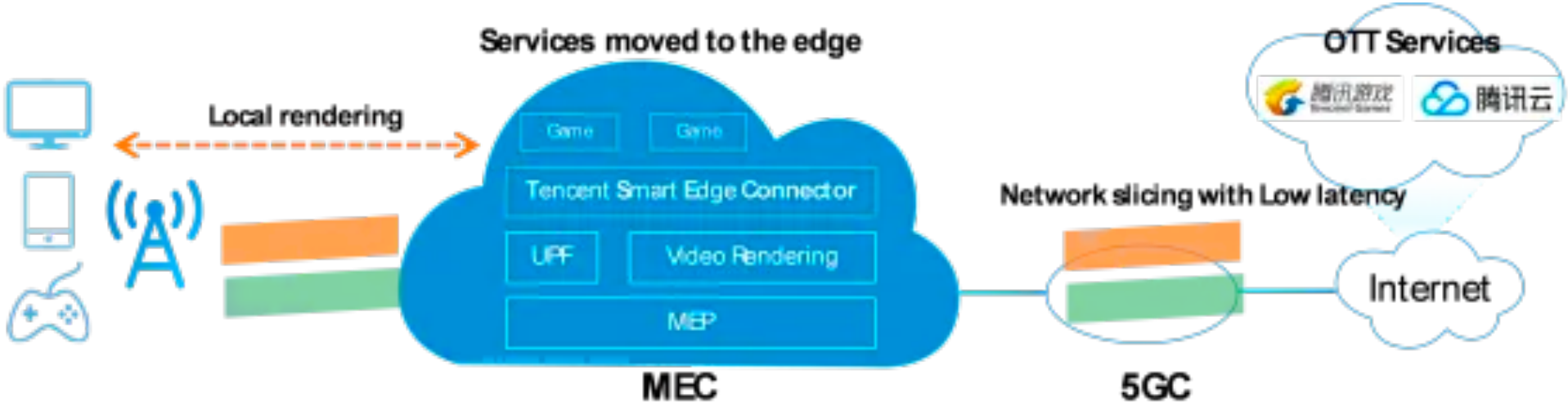
ARCHITECTURE

There are more: NF (Network Function Repository Function) etc...

Virtualisation

- Network function virtualisation
- Like a cloud
  - Scalability
  - Flexibility

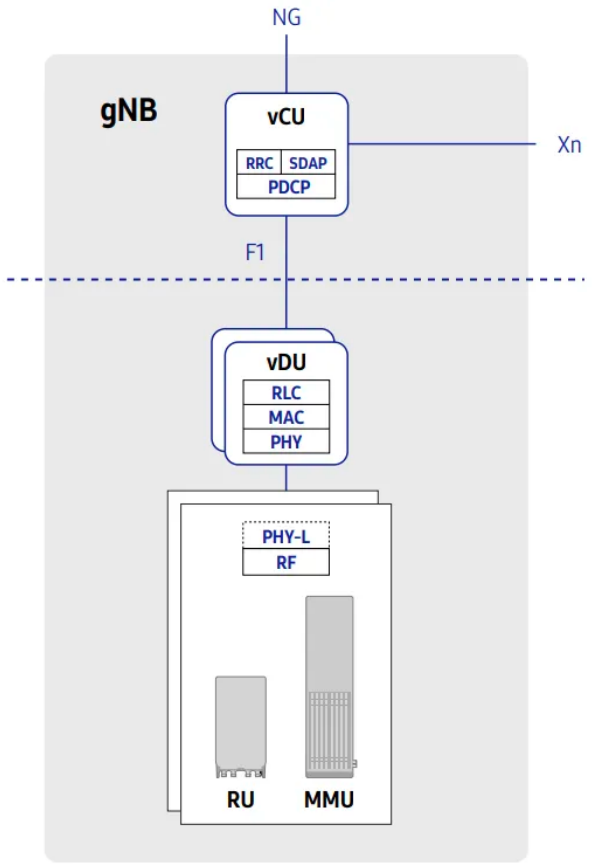
Edge Computing

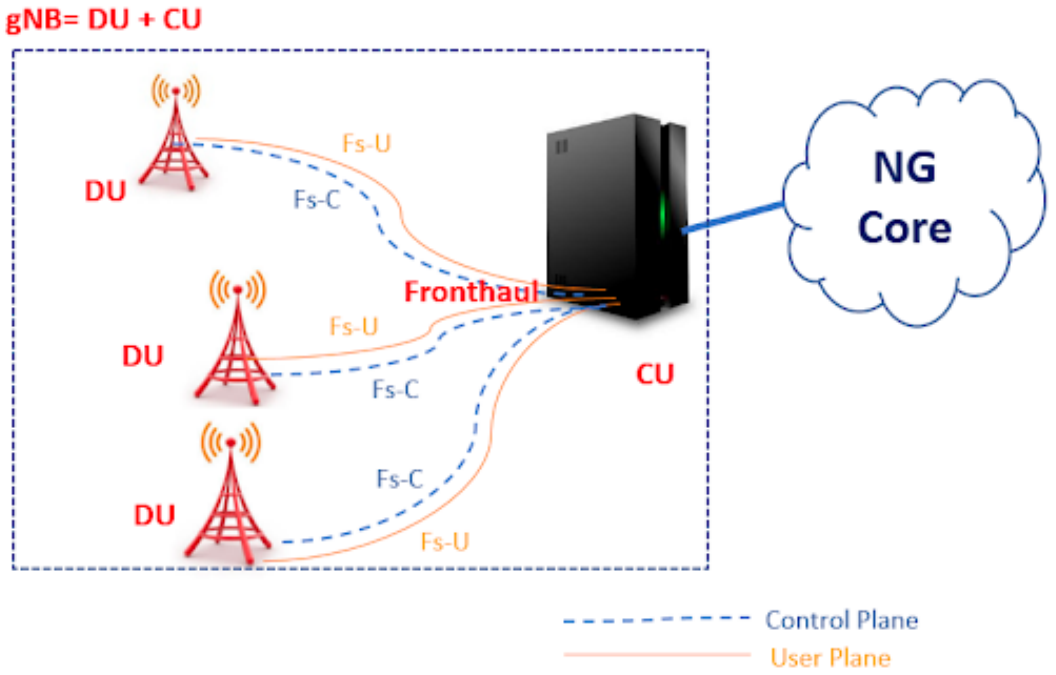


- Ref: https://www.gsma.com/futurenetworks/wiki/5g-mec-based-cloud-game-innovation-practice/

Disaggregation

gNB can be split



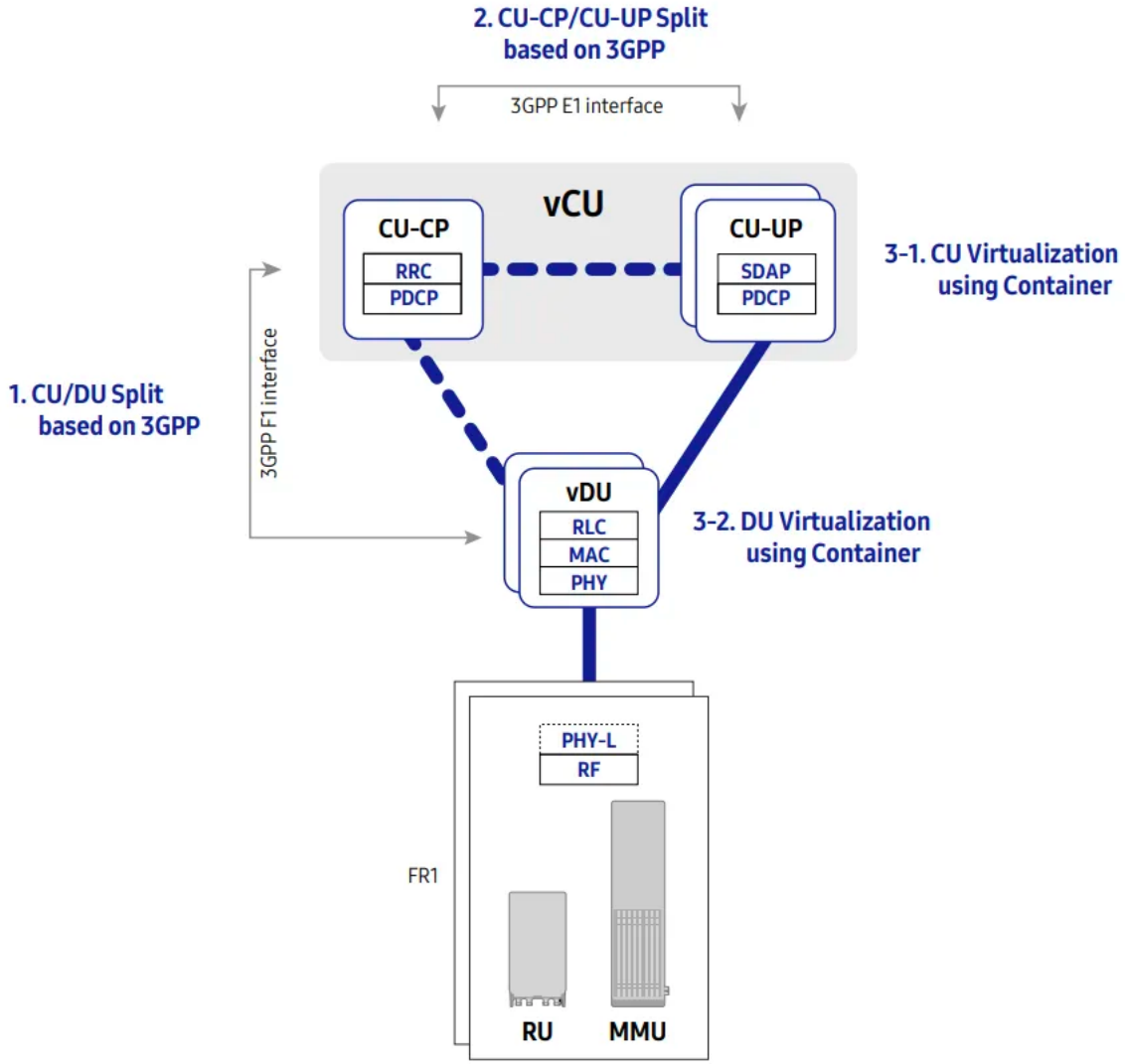


Ref: techplayon.com

Ref: https://www.5g-networks.net/5g-technology/virtualised-and-disaggregated-5g-nr-vran-architecture/

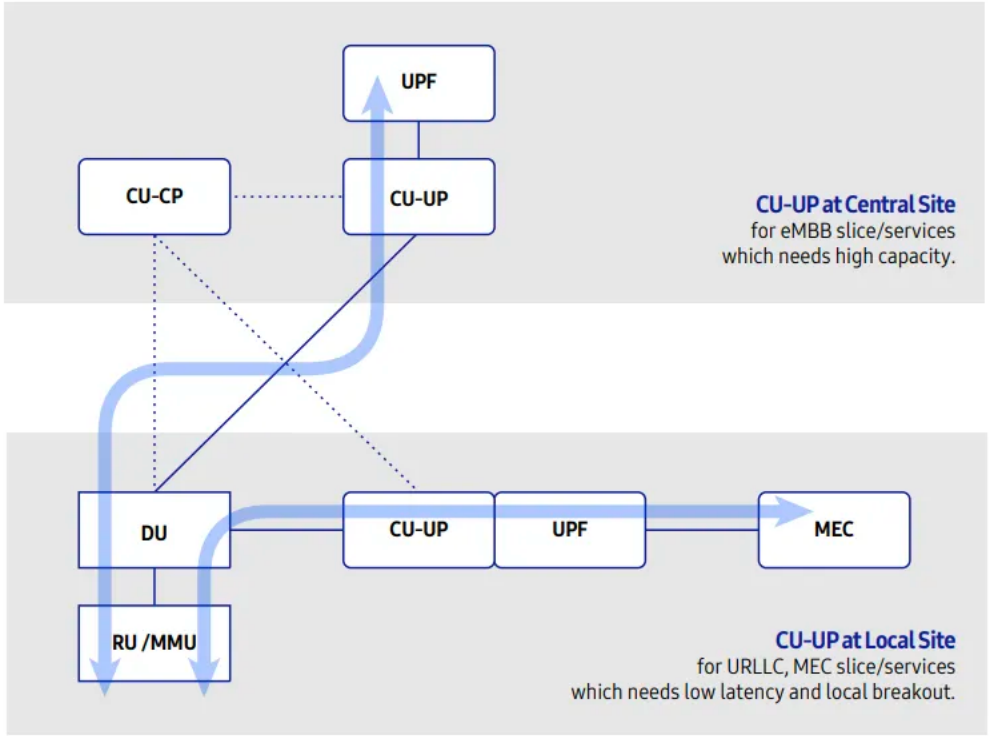
Disaggregation …

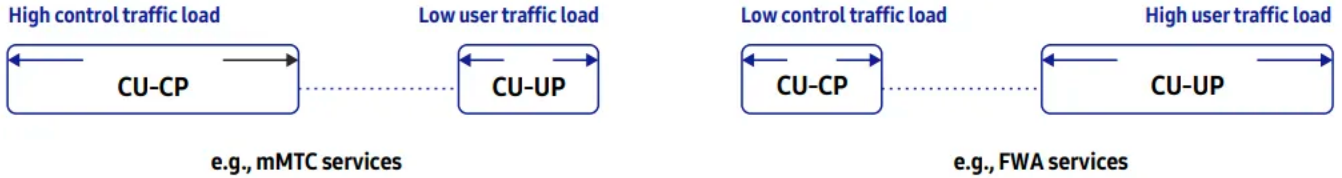
CU can be split



Ref: https://www.5g-networks.net/5g-technology/virtualised-and-disaggregated-5g-nr-vran-architecture/

Disaggregation…





Ref: https://www.5g-networks.net/5g-technology/virtualised-and-disaggregated-5g-nr-vran-architecture/

What next for 5G IoT

- 5G massive IoT
- New Radio Light (NR Light) and advanced power saving
- AI and IoT
- Enhanced ultra-reliable low latency communication (eURLLC)
- Higher precision positioning

Ref: https://www.qualcomm.com/news/onq/2020/05/12/5g-here-whats-next-internet-things

Thanks!